10/500851

FIG. 1

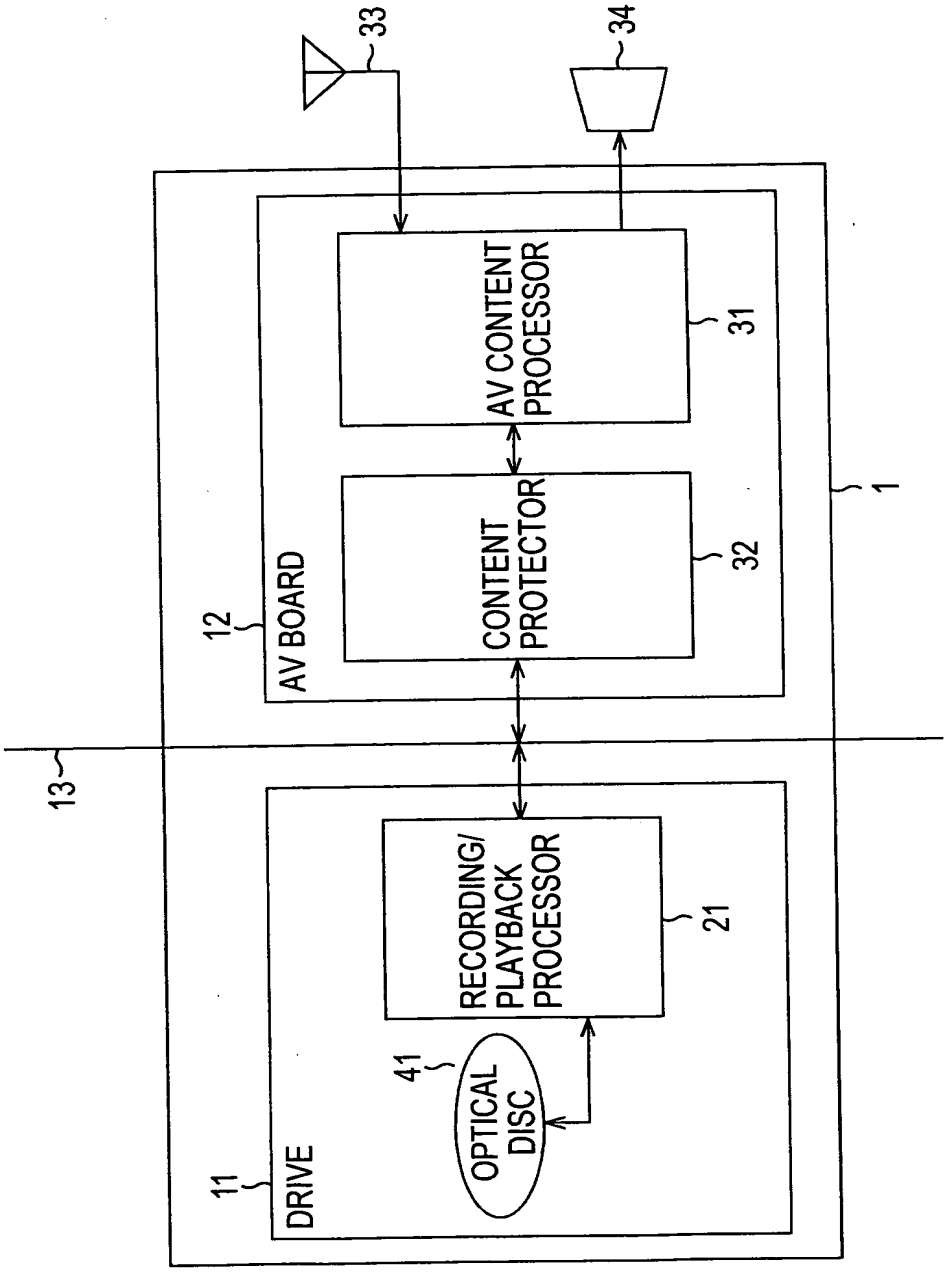


FIG. 2

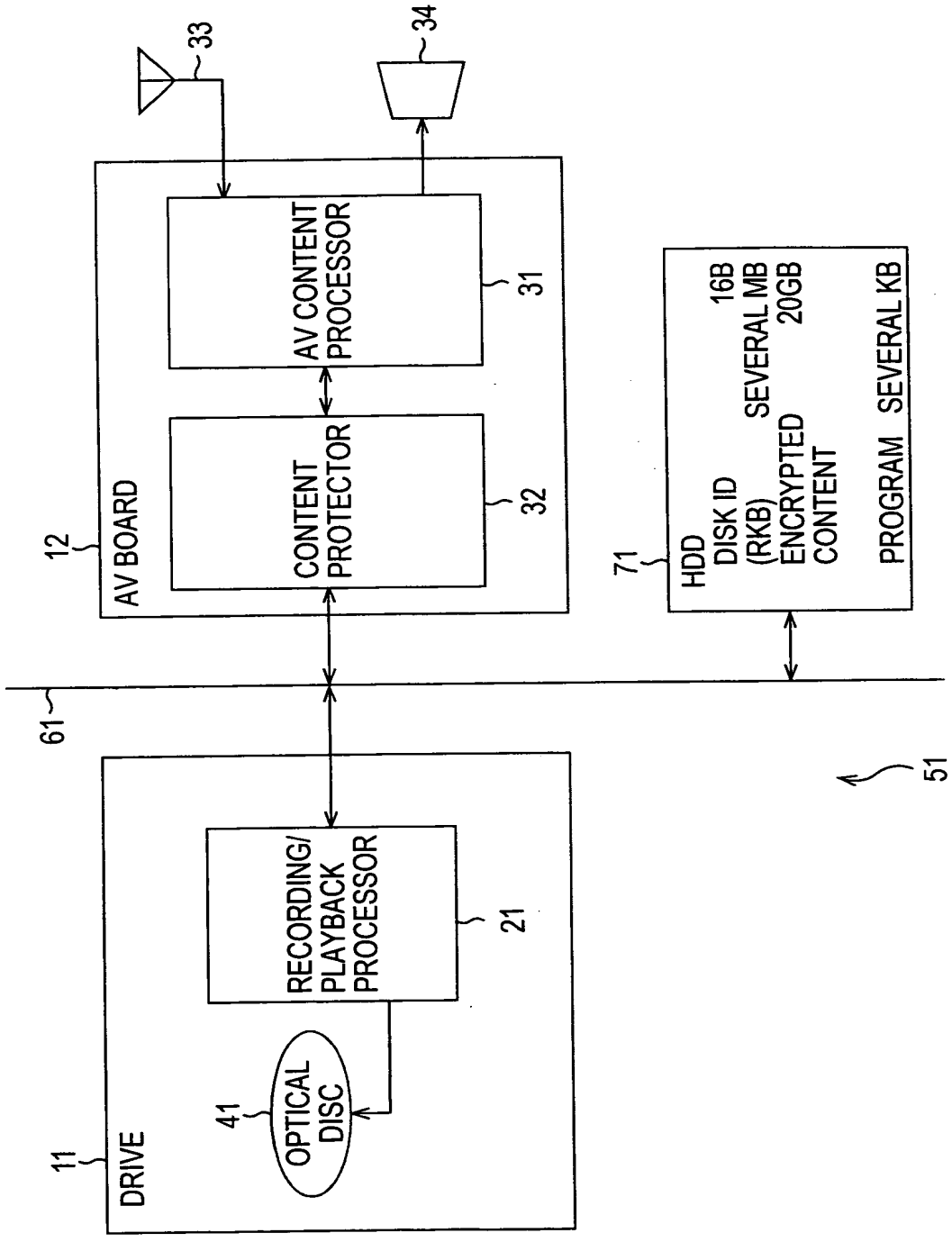

33
34
AV CONTENT PROCESSOR
31
CONTENT PROTECTOR
32
AV BOARD
12
HDD
DISK ID
(RKB)
ENCRYPTED CONTENT
16B
SEVERAL MB
20GB
PROGRAM
SEVERAL KB
71
61
51
RECORDING/ PLAYBACK PROCESSOR
21
OPTICAL DISC
41
DRIVE
11

FIG. 3

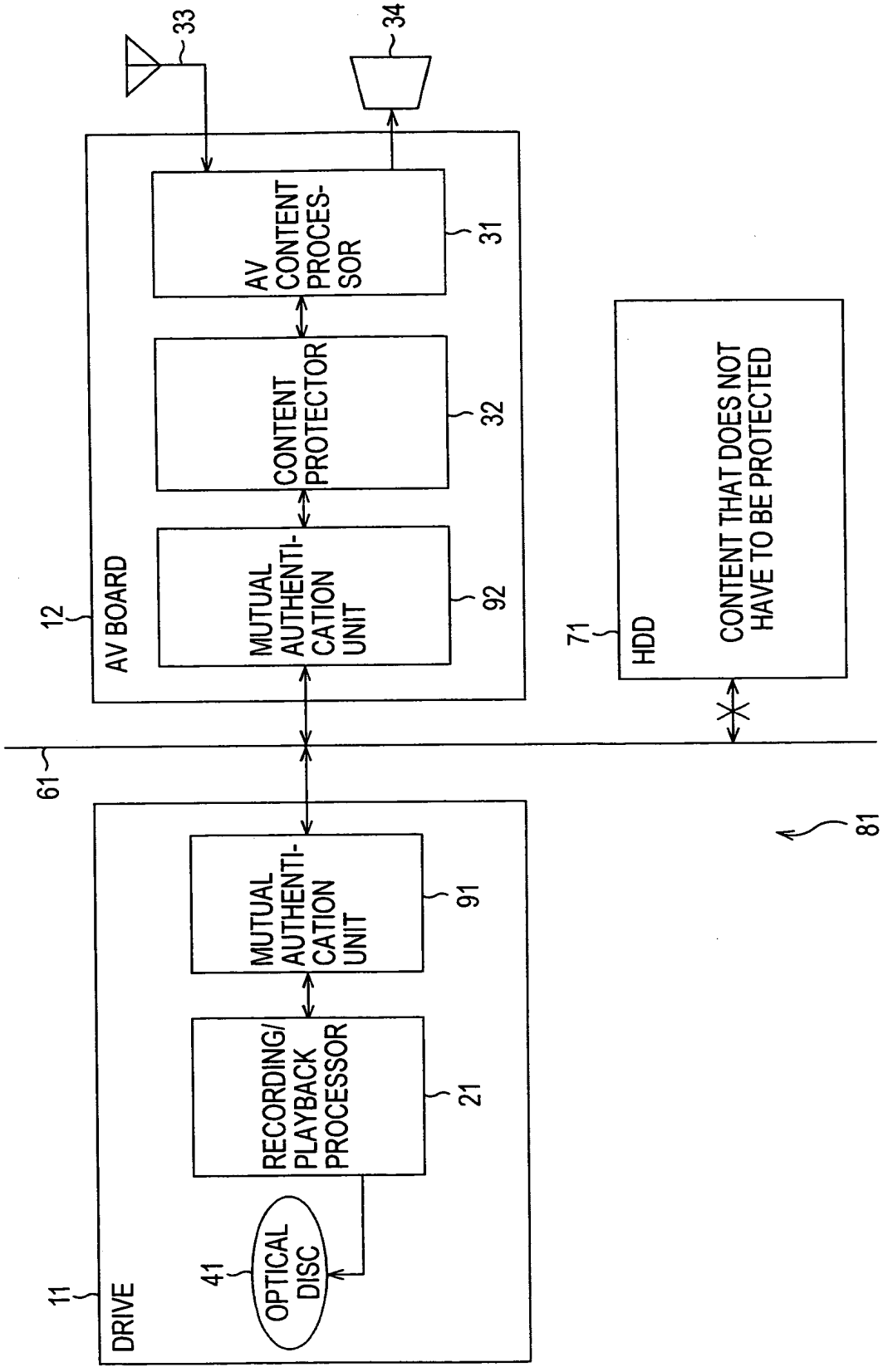

33
34
AV CONTENT PROCES-SOR
31
CONTENT PROTECTOR
32
MUTUAL AUTHENTI-CATION UNIT
92
12
AV BOARD
71
HDD
CONTENT THAT DOES NOT HAVE TO BE PROTECTED
61
81
MUTUAL AUTHENTI-CATION UNIT
91
RECORDING/ PLAYBACK PROCESSOR
21
41
OPTICAL DISC
11
DRIVE

FIG. 4

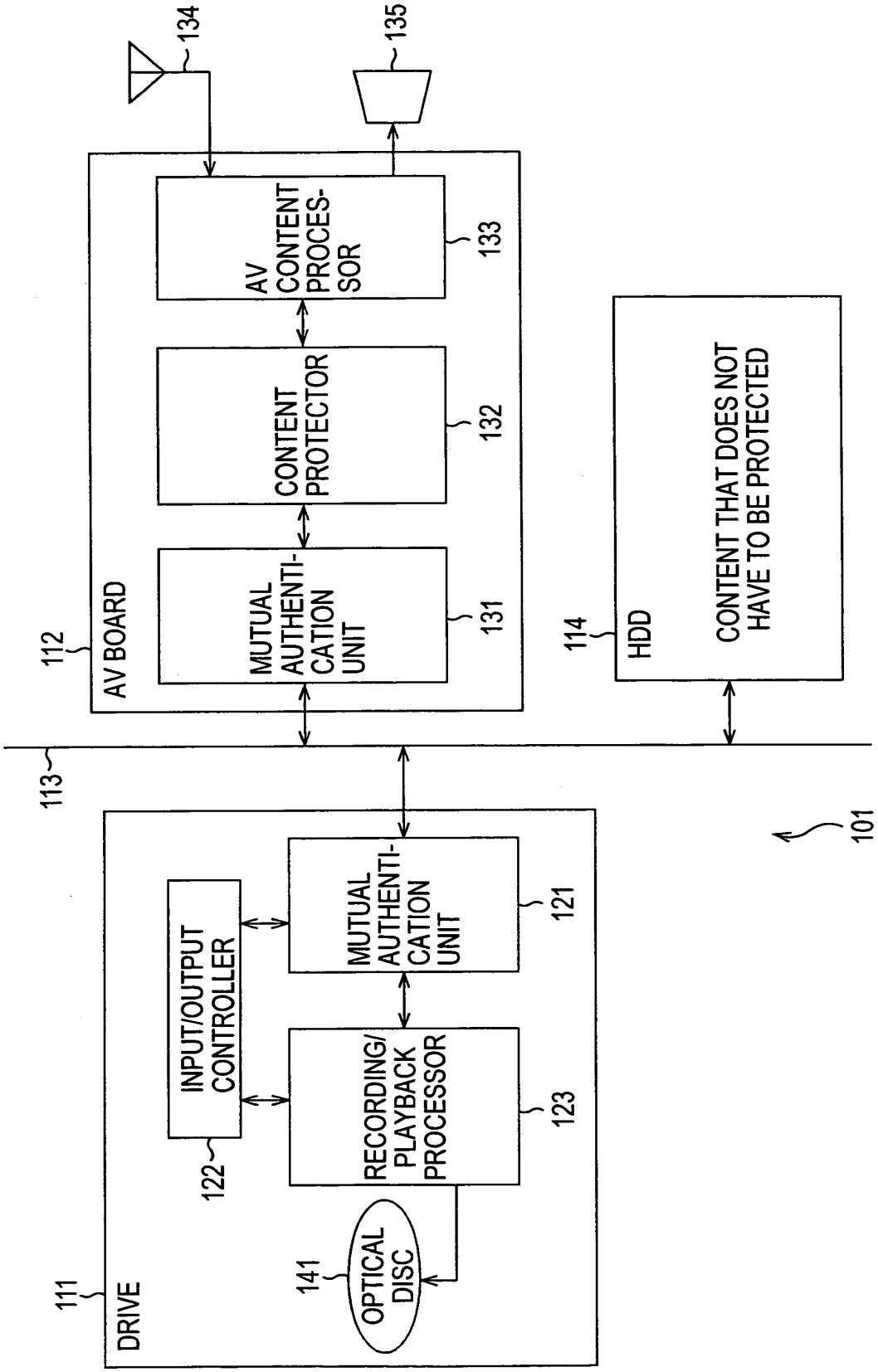

134
135
AV CONTENT PROCES-SOR
133
CONTENT PROTECTOR
132
MUTUAL AUTHENTI-CATION UNIT
131
112
AV BOARD
114
HDD
CONTENT THAT DOES NOT HAVE TO BE PROTECTED
113
101
INPUT/OUTPUT CONTROLLER
122
MUTUAL AUTHENTI-CATION UNIT
121
RECORDING/ PLAYBACK PROCESSOR
123
141
OPTICAL DISC
111
DRIVE

FIG. 5

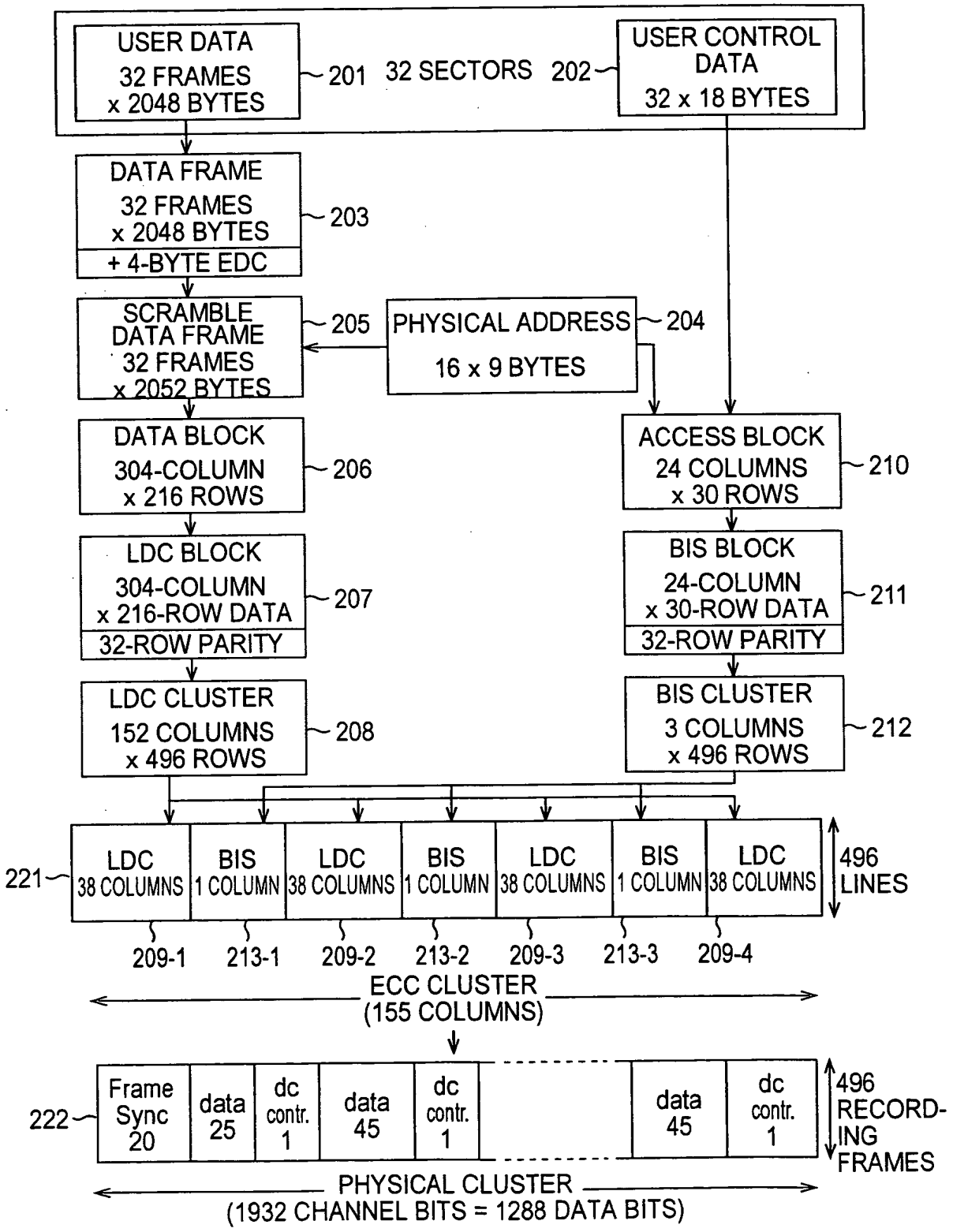

USER DATA
32 FRAMES
x 2048 BYTES
201
32 SECTORS
202
USER CONTROL DATA
32 x 18 BYTES
DATA FRAME
32 FRAMES
x 2048 BYTES
+ 4-BYTE EDC
203
SCRAMBLE DATA FRAME
32 FRAMES
x 2052 BYTES
205
PHYSICAL ADDRESS
16 x 9 BYTES
204
DATA BLOCK
304-COLUMN
x 216 ROWS
206
ACCESS BLOCK
24 COLUMNS
x 30 ROWS
210
LDC BLOCK
304-COLUMN
x 216-ROW DATA
32-ROW PARITY
207
BIS BLOCK
24-COLUMN
x 30-ROW DATA
32-ROW PARITY
211
LDC CLUSTER
152 COLUMNS
x 496 ROWS
208
BIS CLUSTER
3 COLUMNS
x 496 ROWS
212
221
LDC 38 COLUMNS
BIS 1 COLUMN
LDC 38 COLUMNS
BIS 1 COLUMN
LDC 38 COLUMNS
BIS 1 COLUMN
LDC 38 COLUMNS
496 LINES
209-1
213-1
209-2
213-2
209-3
213-3
209-4
ECC CLUSTER
(155 COLUMNS)
222
Frame Sync 20
data 25
dc contr. 1
data 45
dc contr. 1
data 45
dc contr. 1
496 RECORD-ING FRAMES
PHYSICAL CLUSTER
(1932 CHANNEL BITS = 1288 DATA BITS)

FIG. 6

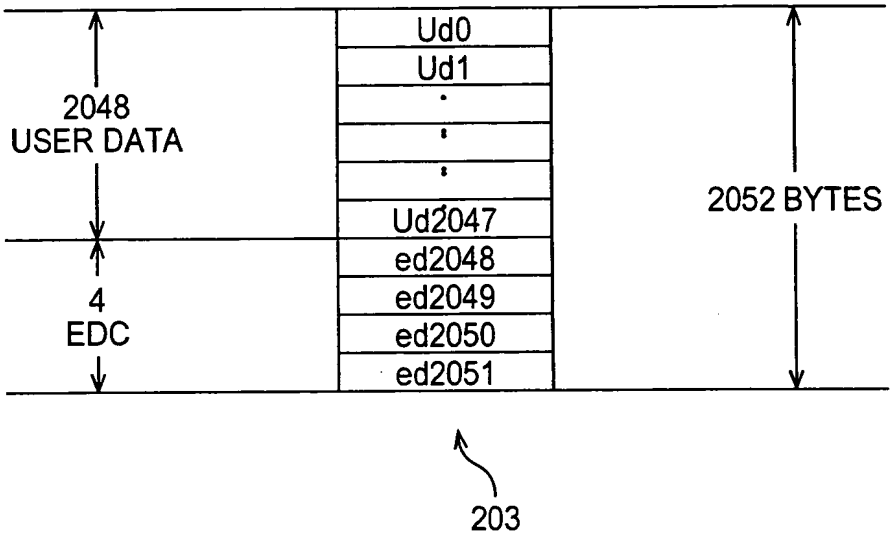

2048
USER DATA
4
EDC
Ud0
Ud1
Ud2047
ed2048
ed2049
ed2050
ed2051
2052 BYTES
203

FIG. 7

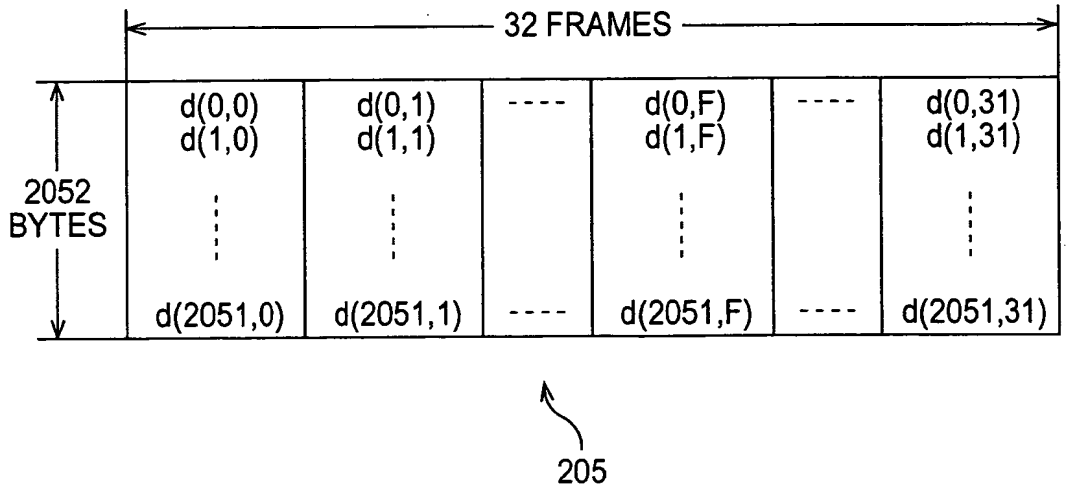
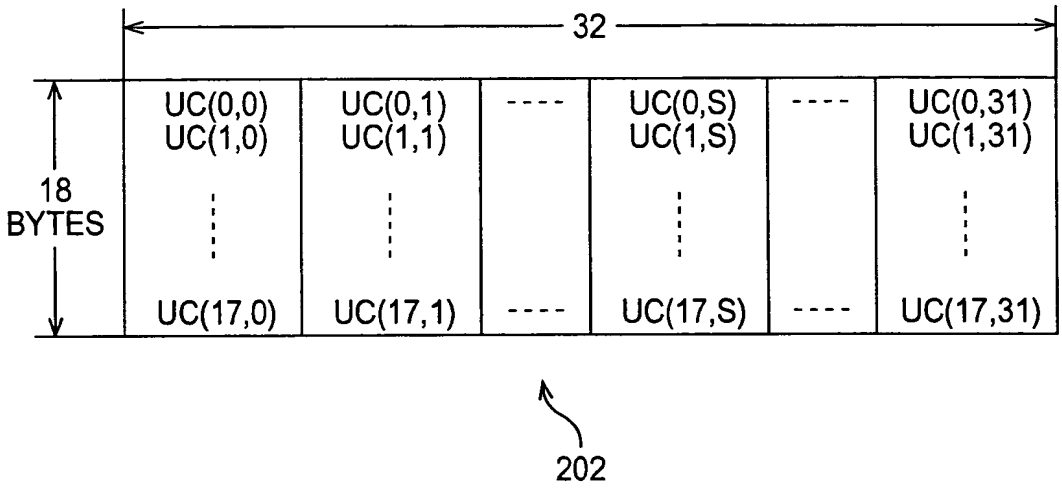

32 FRAMES
2052
BYTES
d(0,0)
d(1,0)
d(0,1)
d(1,1)
d(0,F)
d(1,F)
d(0,31)
d(1,31)
d(2051,0)
d(2051,1)
d(2051,F)
d(2051,31)
205

FIG. 8


32
18 BYTES
UC(0,0)
UC(1,0)
UC(0,1)
UC(1,1)

UC(0,S)
UC(1,S)

UC(0,31)
UC(1,31)
UC(17,0)
UC(17,1)

UC(17,S)

UC(17,31)
202

FIG. 9

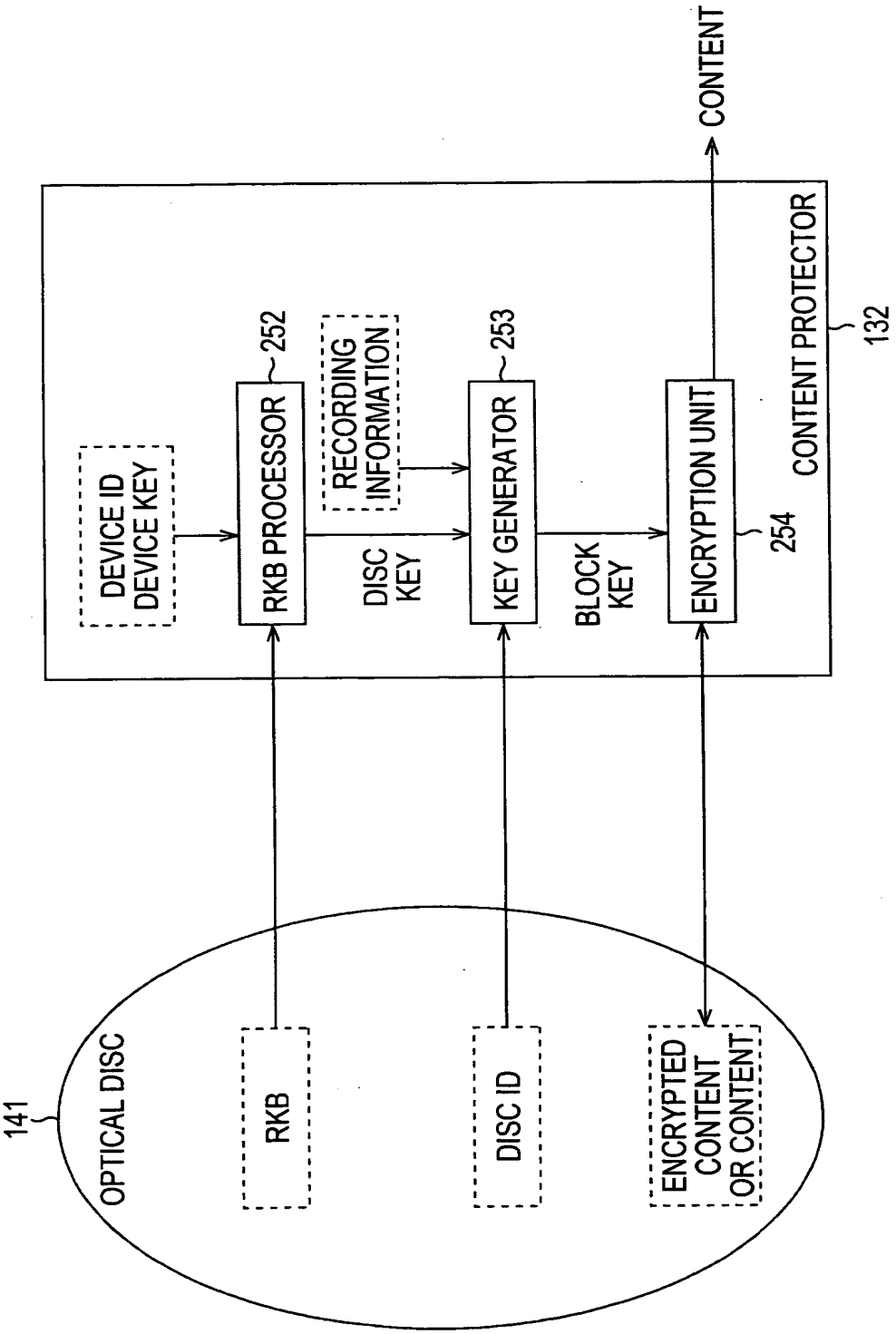

CONTENT
CONTENT PROTECTOR
132
DEVICE ID
DEVICE KEY
RKB PROCESSOR
252
RECORDING
INFORMATION
DISC
KEY
KEY GENERATOR
253
BLOCK
KEY
ENCRYPTION UNIT
254
141
OPTICAL DISC
RKB
DISC ID
ENCRYPTED
CONTENT
OR CONTENT

FIG. 10

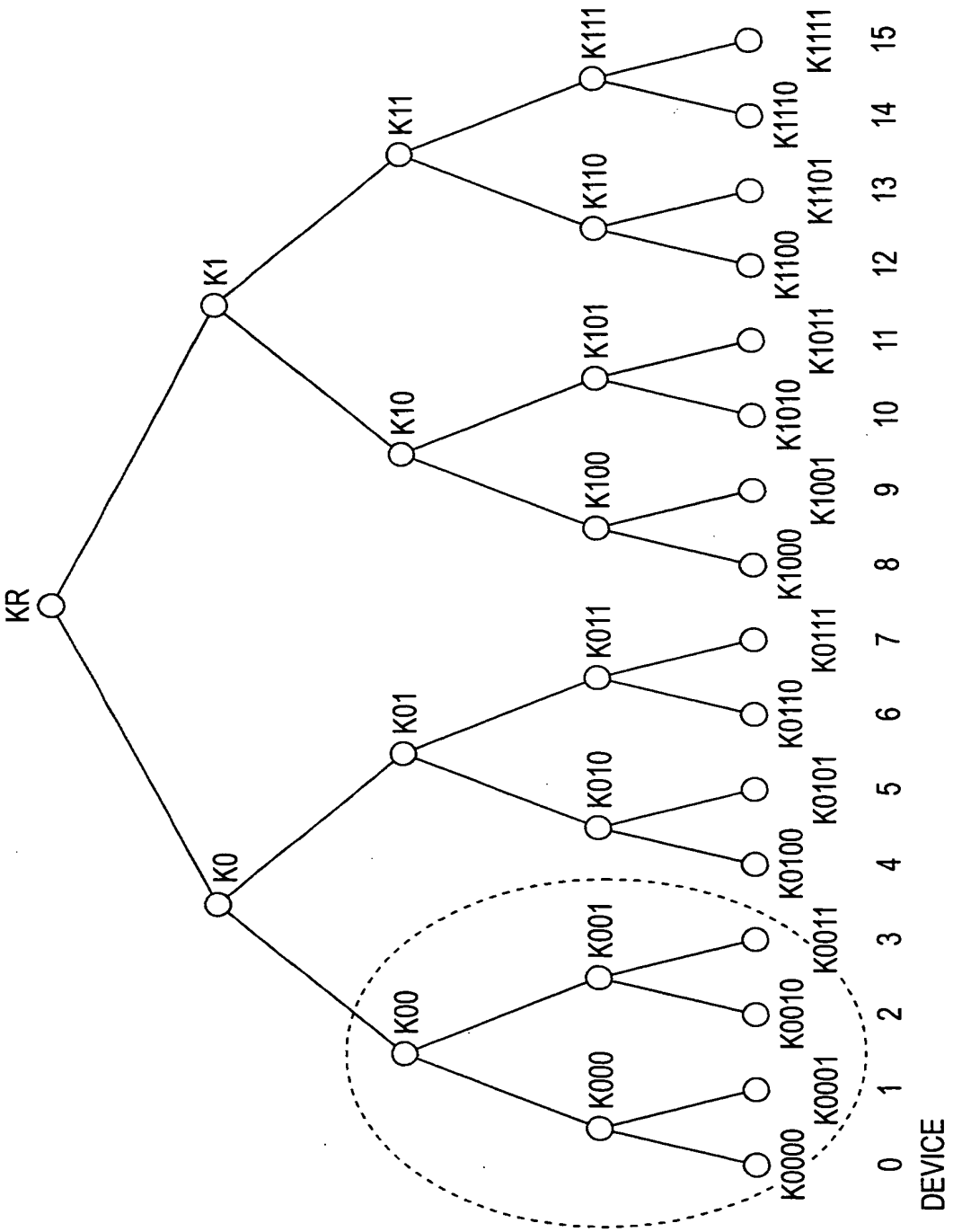

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
DEVICE

FIG. 11A

VERSION(Version):t	
INDEX	ENCRYPTED KEY
0	Enc(K(t)0,K(t)R)
00	Enc(K(t)00,K(t)0)
000	Enc(K000,K(t)00)
001	Enc(K(t)001,K(t)00)
0010	Enc(K0010,K(t)001)

FIG. 11B

VERSION(Version):t	
INDEX	ENCRYPTED KEY
000	Enc(K000,K(t)00)
001	Enc(K(t)001,K(t)00)
0010	Enc(K0010,K(t)001)

FIG. 12

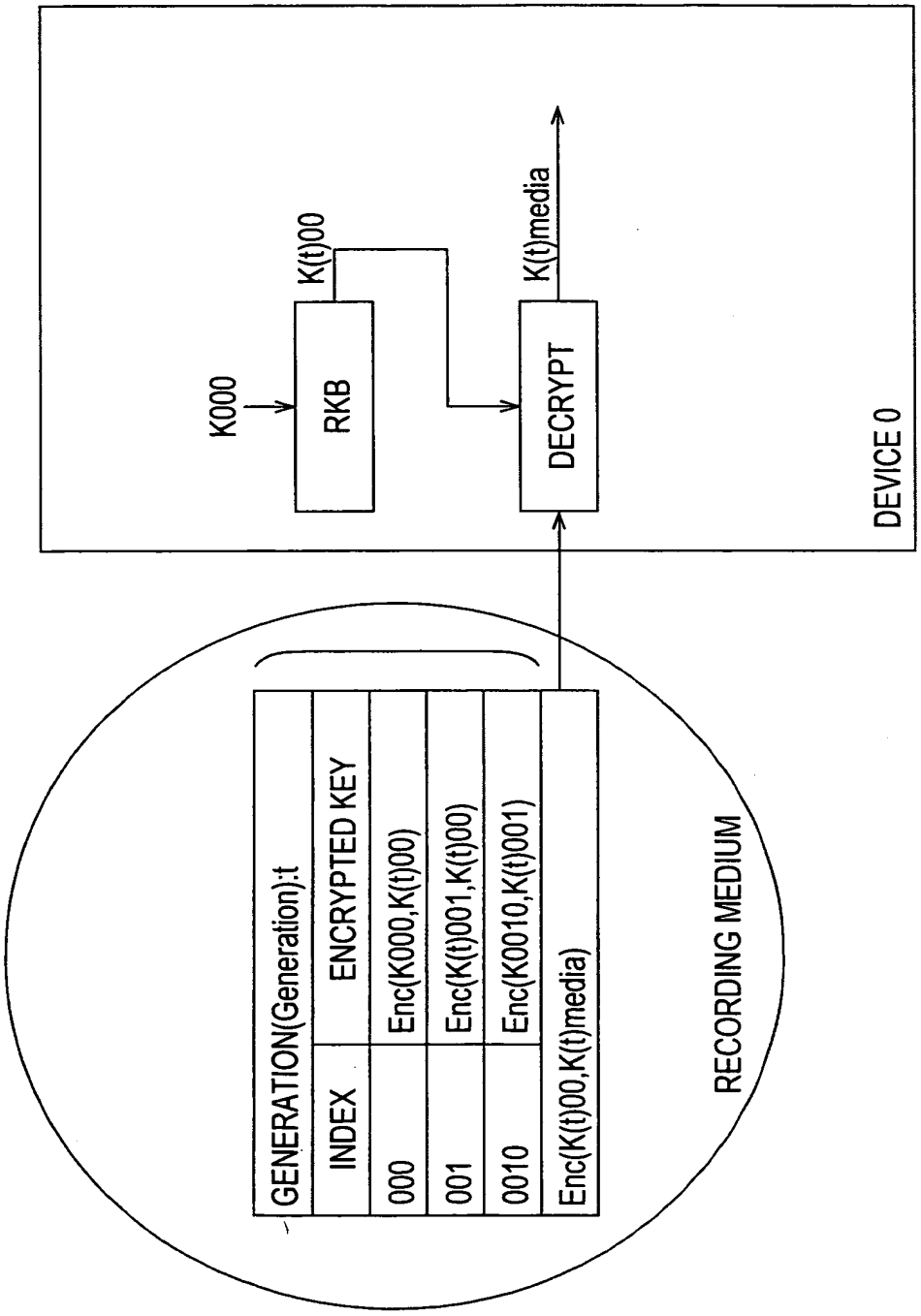

DEVICE 0
K000
RKB
K(t)00
DECRYPT
K(t)media
RECORDING MEDIUM
GENERATION(Generation):t
INDEX
ENCRYPTED KEY
000
Enc(K000,K(t)00)
001
Enc(K(t)001,K(t)00)
0010
Enc(K0010,K(t)001)
Enc(K(t)00,K(t)media)

FIG. 13

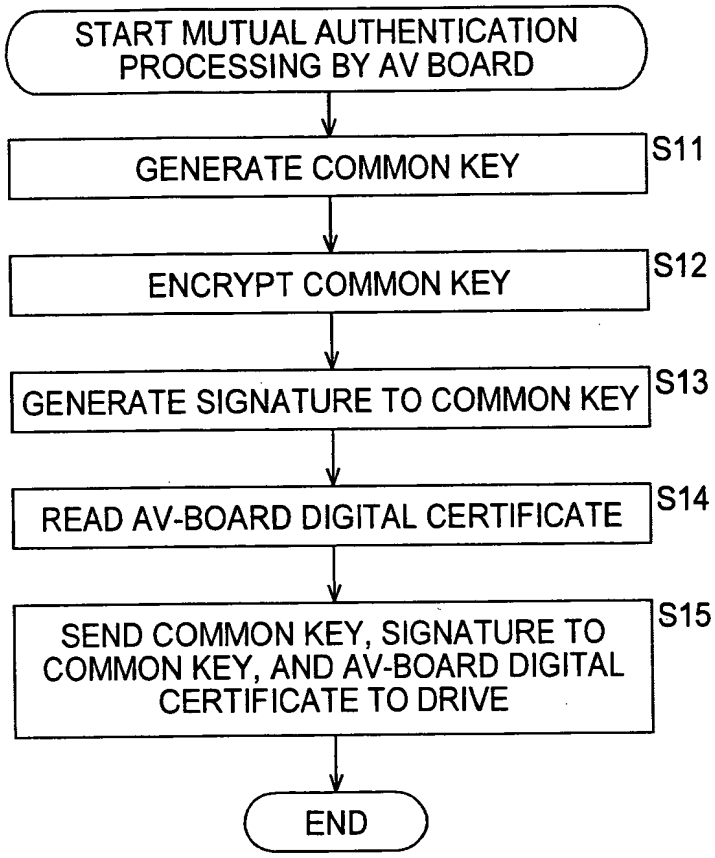

START MUTUAL AUTHENTICATION PROCESSING BY AV BOARD
GENERATE COMMON KEY
S11
ENCRYPT COMMON KEY
S12
GENERATE SIGNATURE TO COMMON KEY
S13
READ AV-BOARD DIGITAL CERTIFICATE
S14
SEND COMMON KEY, SIGNATURE TO COMMON KEY, AND AV-BOARD DIGITAL CERTIFICATE TO DRIVE
S15
END

FIG. 14

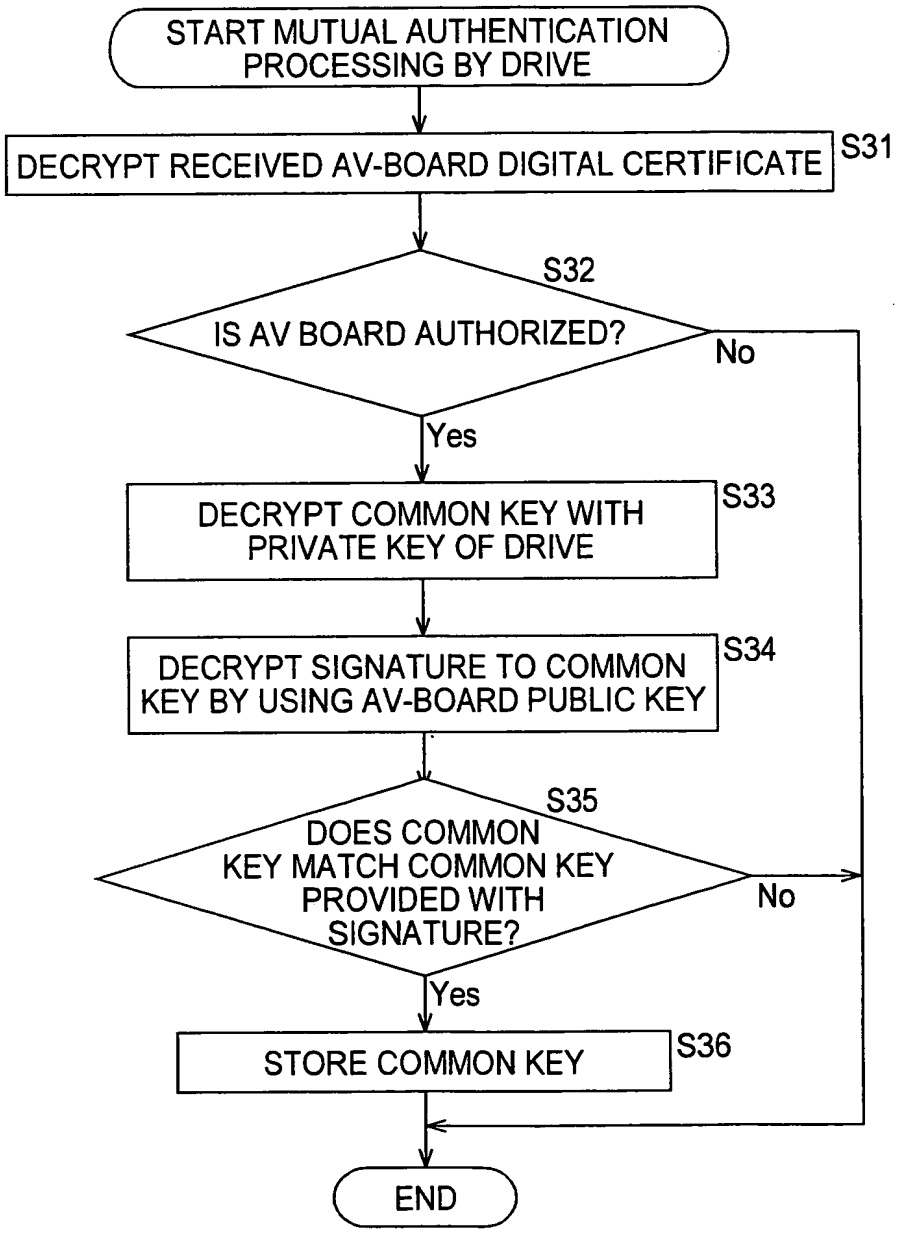

START MUTUAL AUTHENTICATION PROCESSING BY DRIVE
DECRYPT RECEIVED AV-BOARD DIGITAL CERTIFICATE
S31
S32
IS AV BOARD AUTHORIZED?
No
Yes
DECRYPT COMMON KEY WITH PRIVATE KEY OF DRIVE
S33
DECRYPT SIGNATURE TO COMMON KEY BY USING AV-BOARD PUBLIC KEY
S34
S35
DOES COMMON KEY MATCH COMMON KEY PROVIDED WITH SIGNATURE?
No
Yes
STORE COMMON KEY
S36
END

FIG. 15

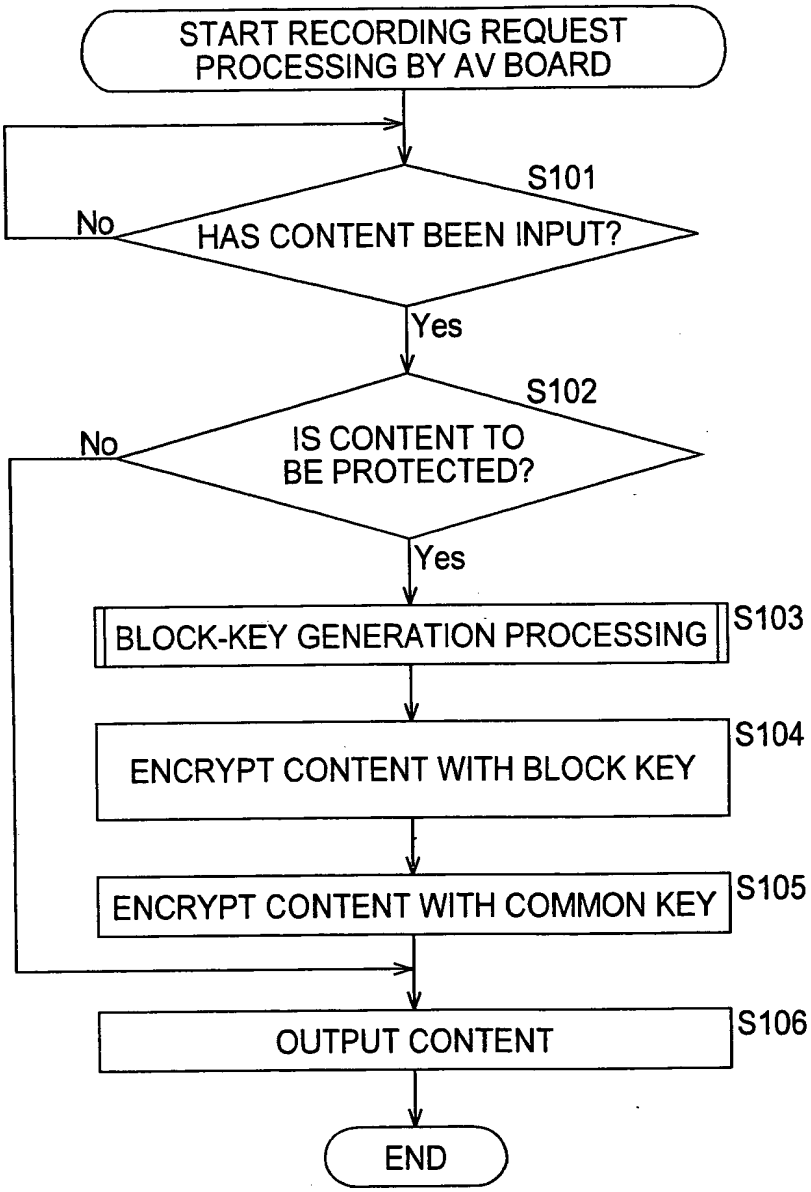

START RECORDING REQUEST PROCESSING BY AV BOARD
S101
No
HAS CONTENT BEEN INPUT?
Yes
S102
No
IS CONTENT TO BE PROTECTED?
Yes
BLOCK-KEY GENERATION PROCESSING
S103
ENCRYPT CONTENT WITH BLOCK KEY
S104
ENCRYPT CONTENT WITH COMMON KEY
S105
OUTPUT CONTENT
S106
END

FIG. 16

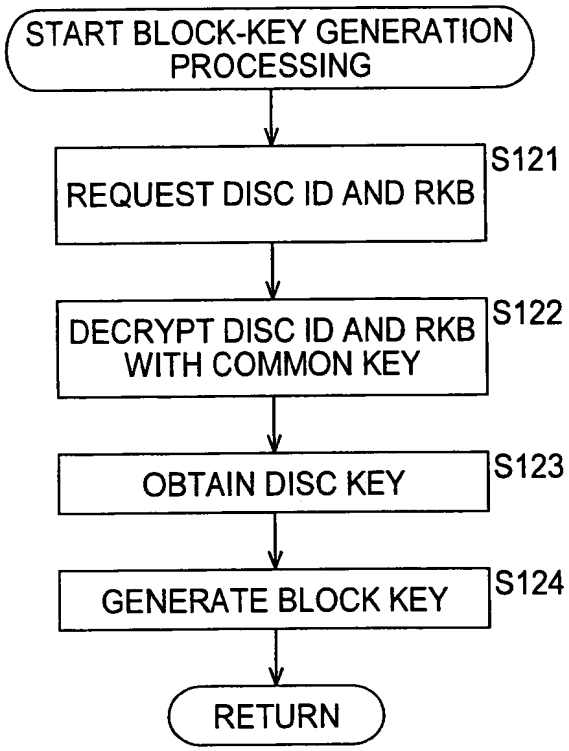

START BLOCK-KEY GENERATION PROCESSING
REQUEST DISC ID AND RKB
S121
DECRYPT DISC ID AND RKB WITH COMMON KEY
S122
OBTAIN DISC KEY
S123
GENERATE BLOCK KEY
S124
RETURN

FIG. 17

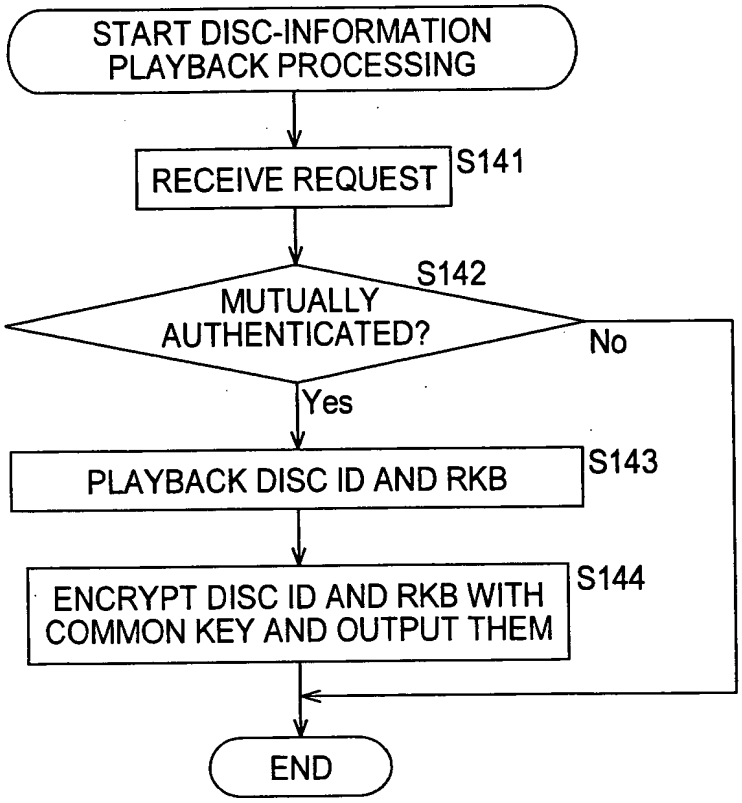

START DISC-INFORMATION PLAYBACK PROCESSING
RECEIVE REQUEST
S141
S142
MUTUALLY AUTHENTICATED?
No
Yes
PLAYBACK DISC ID AND RKB
S143
ENCRYPT DISC ID AND RKB WITH COMMON KEY AND OUTPUT THEM
S144
END

FIG. 18

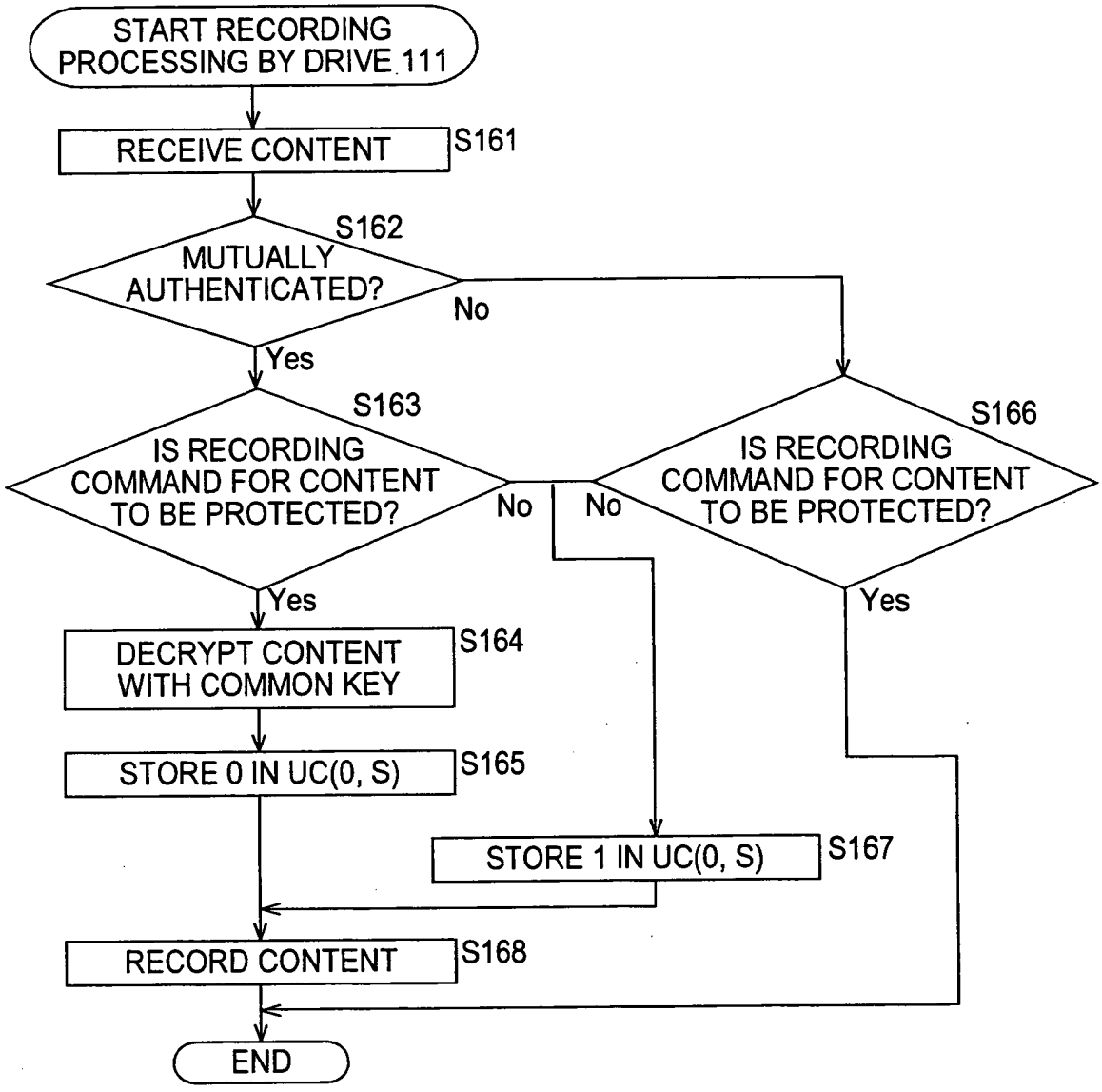

START RECORDING PROCESSING BY DRIVE 111
RECEIVE CONTENT
S161
S162
MUTUALLY AUTHENTICATED?
No
Yes
S163
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
S166
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
DECRYPT CONTENT WITH COMMON KEY
S164
STORE 0 IN UC(0, S)
S165
STORE 1 IN UC(0, S)
S167
RECORD CONTENT
S168
END

FIG. 19

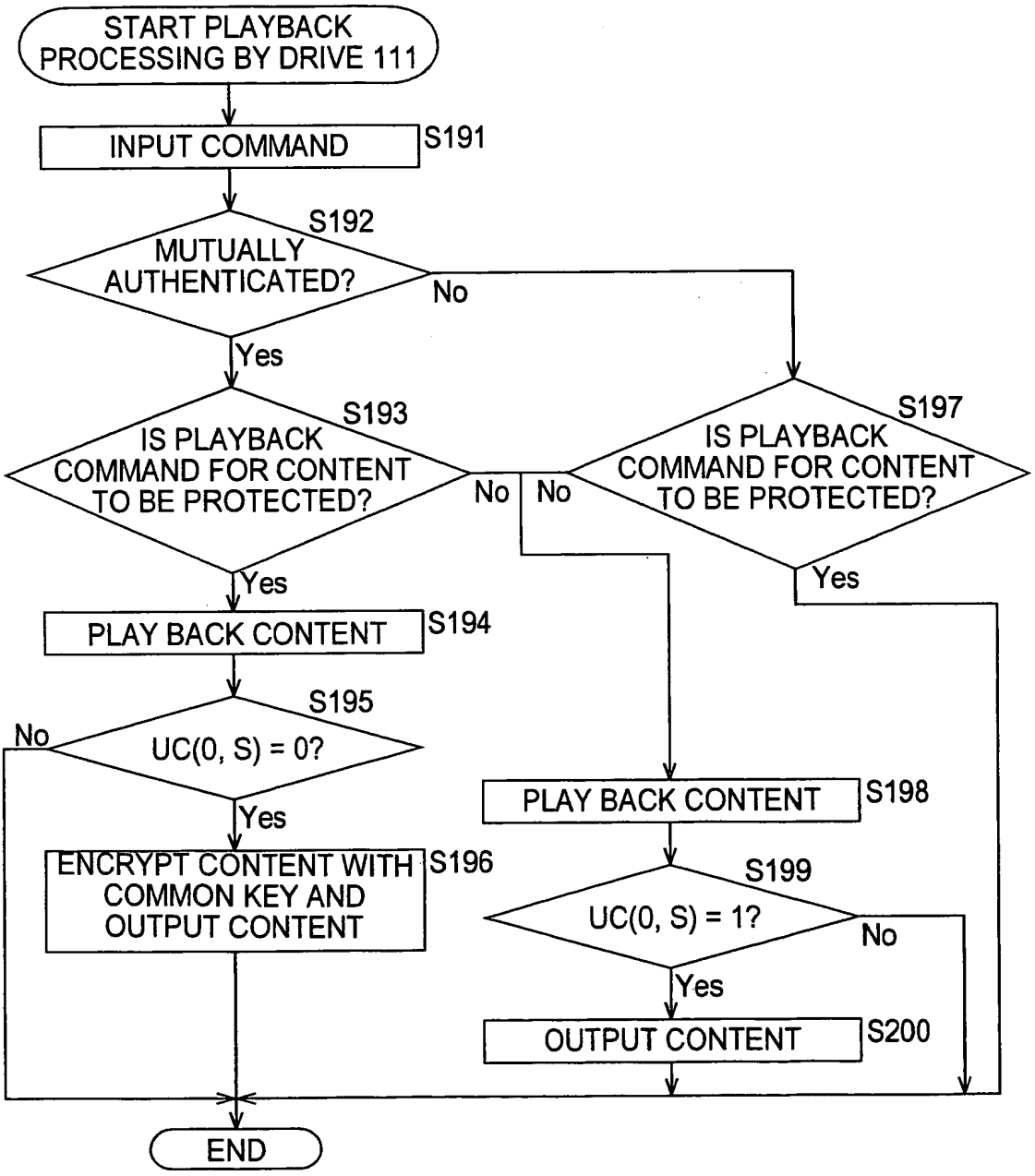

START PLAYBACK PROCESSING BY DRIVE 111
INPUT COMMAND
S191
S192
MUTUALLY AUTHENTICATED?
No
Yes
S193
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
S197
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
PLAY BACK CONTENT
S194
S195
No
UC(0, S) = 0?
Yes
ENCRYPT CONTENT WITH COMMON KEY AND OUTPUT CONTENT
S196
PLAY BACK CONTENT
S198
S199
UC(0, S) = 1?
No
Yes
OUTPUT CONTENT
S200
END

FIG. 20

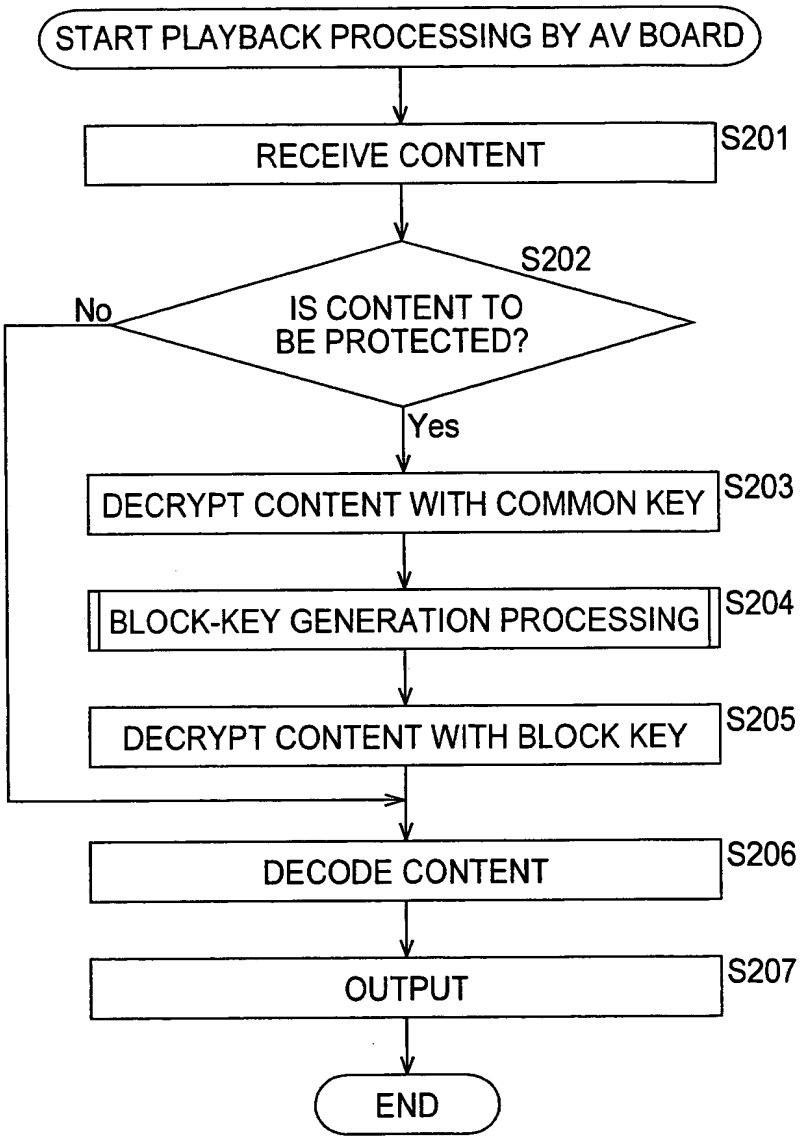

START PLAYBACK PROCESSING BY AV BOARD
RECEIVE CONTENT
S201
S202
IS CONTENT TO BE PROTECTED?
No
Yes
DECRYPT CONTENT WITH COMMON KEY
S203
BLOCK-KEY GENERATION PROCESSING
S204
DECRYPT CONTENT WITH BLOCK KEY
S205
DECODE CONTENT
S206
OUTPUT
S207
END

FIG. 21

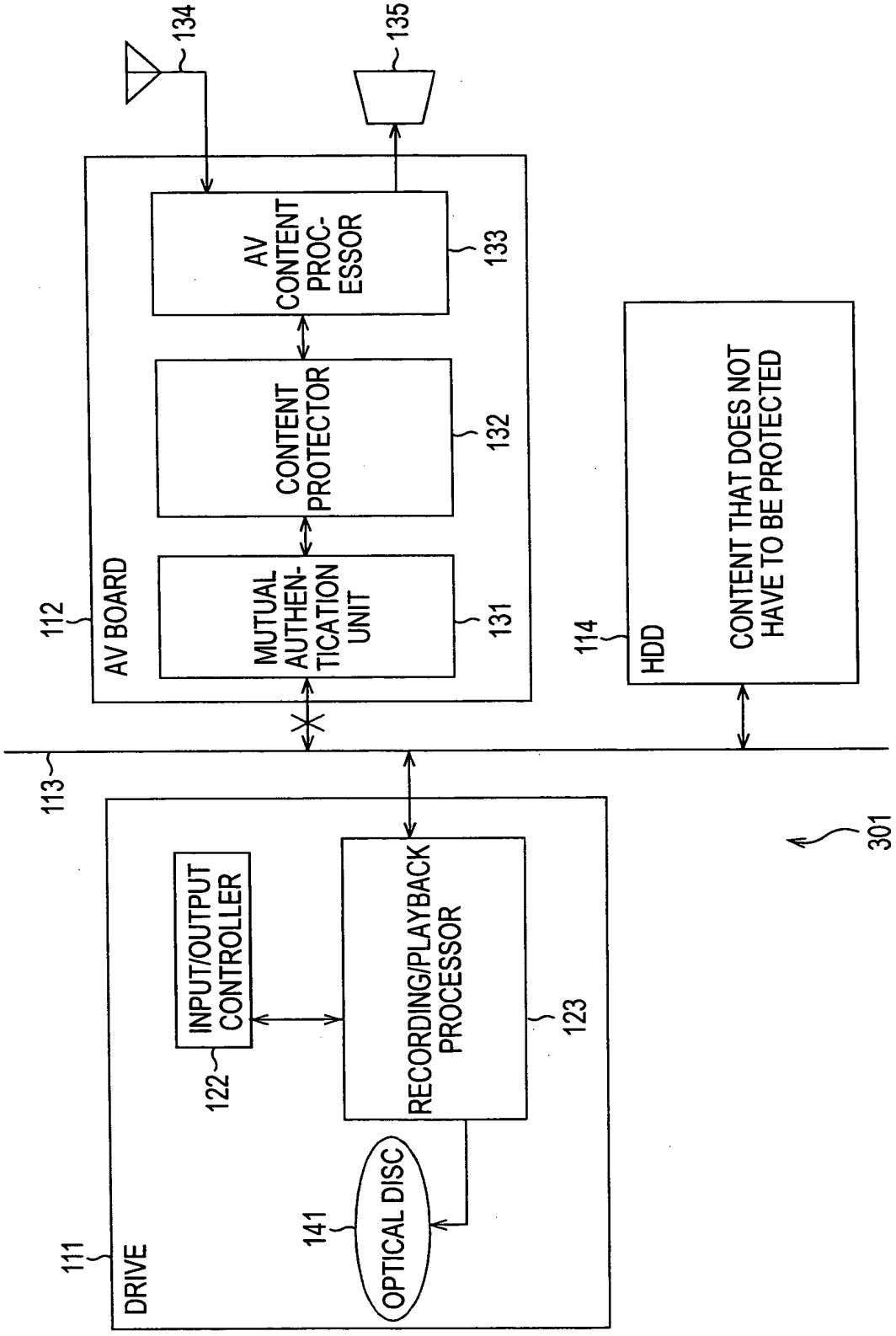

134
135
AV CONTENT PROC-ESSOR
133
CONTENT PROTECTOR
132
MUTUAL AUTHEN-TICATION UNIT
131
112
AV BOARD
114
HDD
CONTENT THAT DOES NOT HAVE TO BE PROTECTED
113
301
INPUT/OUTPUT CONTROLLER
122
RECORDING/PLAYBACK PROCESSOR
123
141
OPTICAL DISC
111
DRIVE

FIG. 22

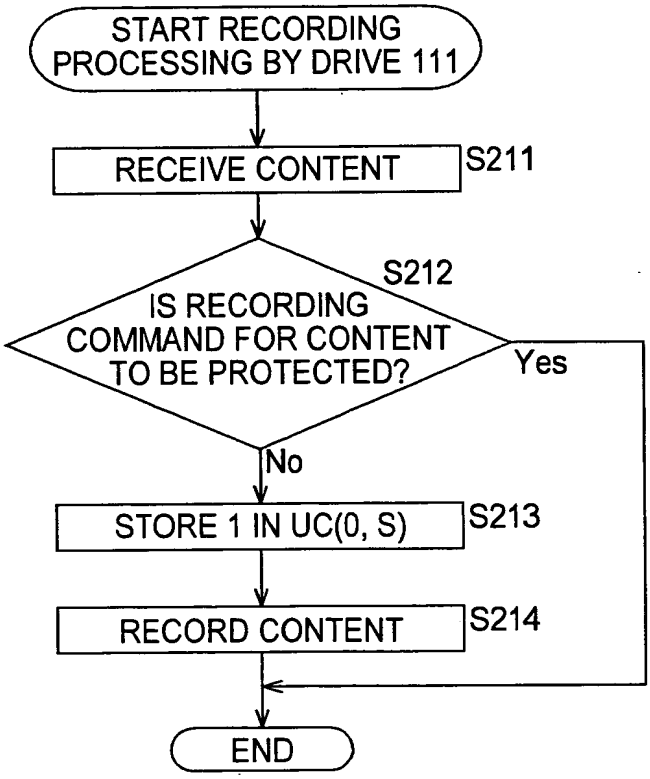

START RECORDING PROCESSING BY DRIVE 111
RECEIVE CONTENT
S211
S212
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
Yes
No
STORE 1 IN UC(0, S)
S213
RECORD CONTENT
S214
END

FIG. 23

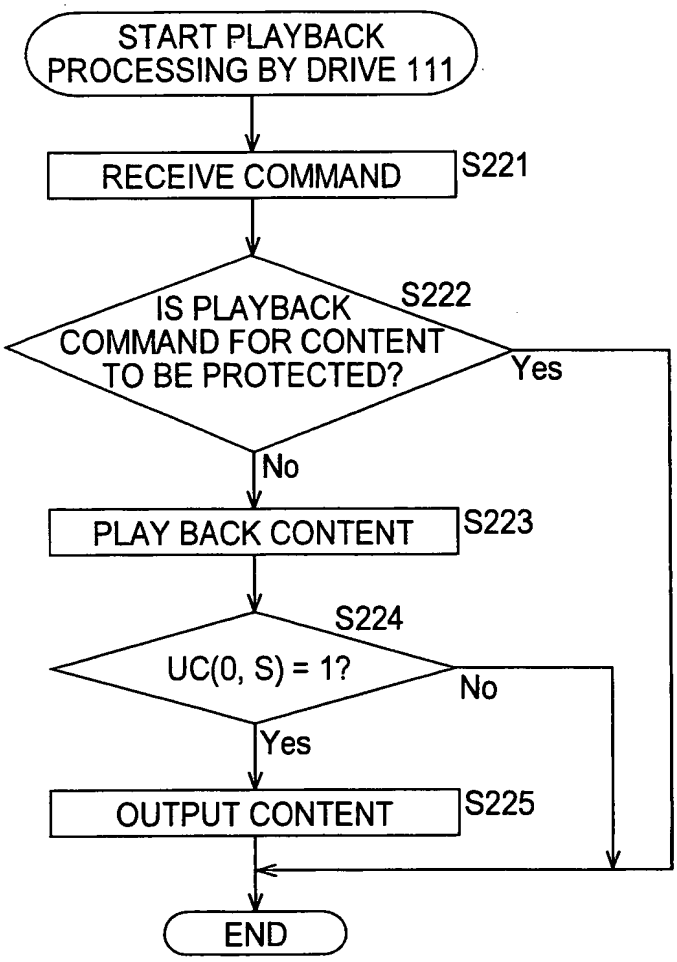

START PLAYBACK PROCESSING BY DRIVE 111
RECEIVE COMMAND
S221
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
S222
Yes
No
PLAY BACK CONTENT
S223
UC(0, S) = 1?
S224
No
Yes
OUTPUT CONTENT
S225
END

FIG. 24

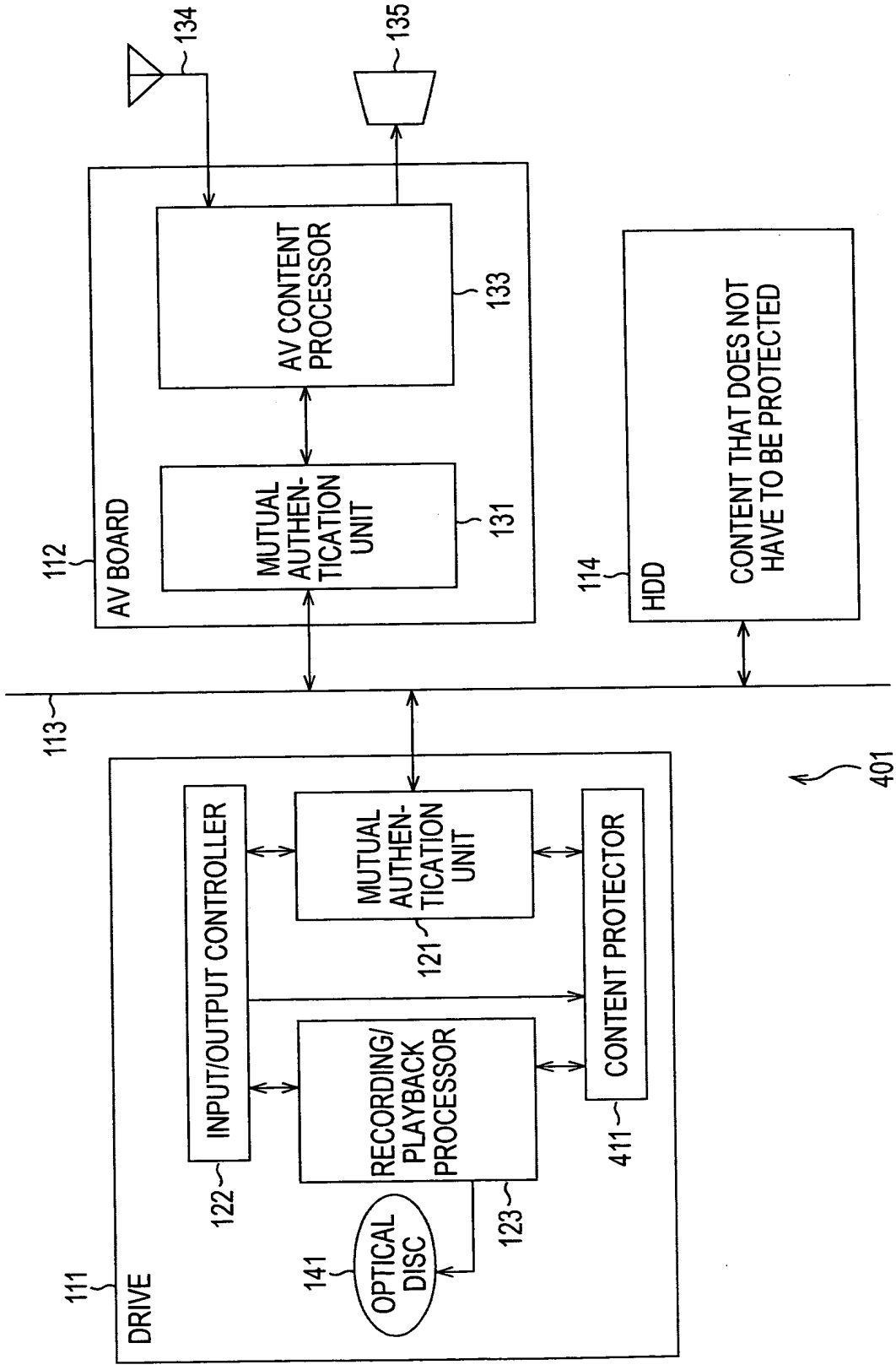

134
135
AV CONTENT PROCESSOR
133
MUTUAL AUTHEN-TICATION UNIT
131
112
AV BOARD
114
HDD
CONTENT THAT DOES NOT HAVE TO BE PROTECTED
113
401
INPUT/OUTPUT CONTROLLER
MUTUAL AUTHEN-TICATION UNIT
121
CONTENT PROTECTOR
RECORDING/ PLAYBACK PROCESSOR
122
123
411
141
OPTICAL DISC
111
DRIVE

FIG. 25

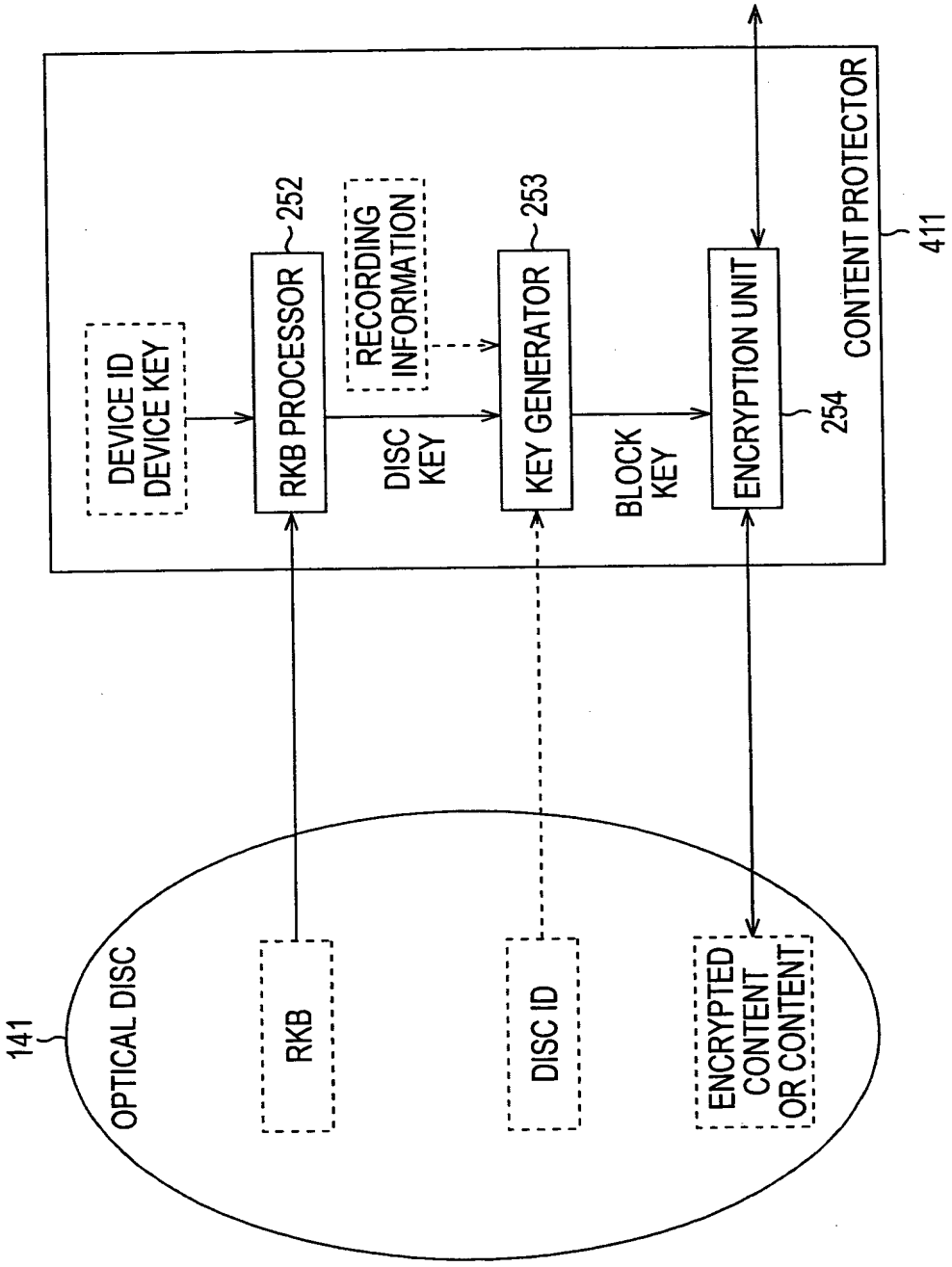

CONTENT PROTECTOR
411
DEVICE ID
DEVICE KEY
RKB PROCESSOR
252
RECORDING INFORMATION
KEY GENERATOR
253
ENCRYPTION UNIT
254
DISC KEY
BLOCK KEY
OPTICAL DISC
141
RKB
DISC ID
ENCRYPTED CONTENT OR CONTENT

FIG. 26

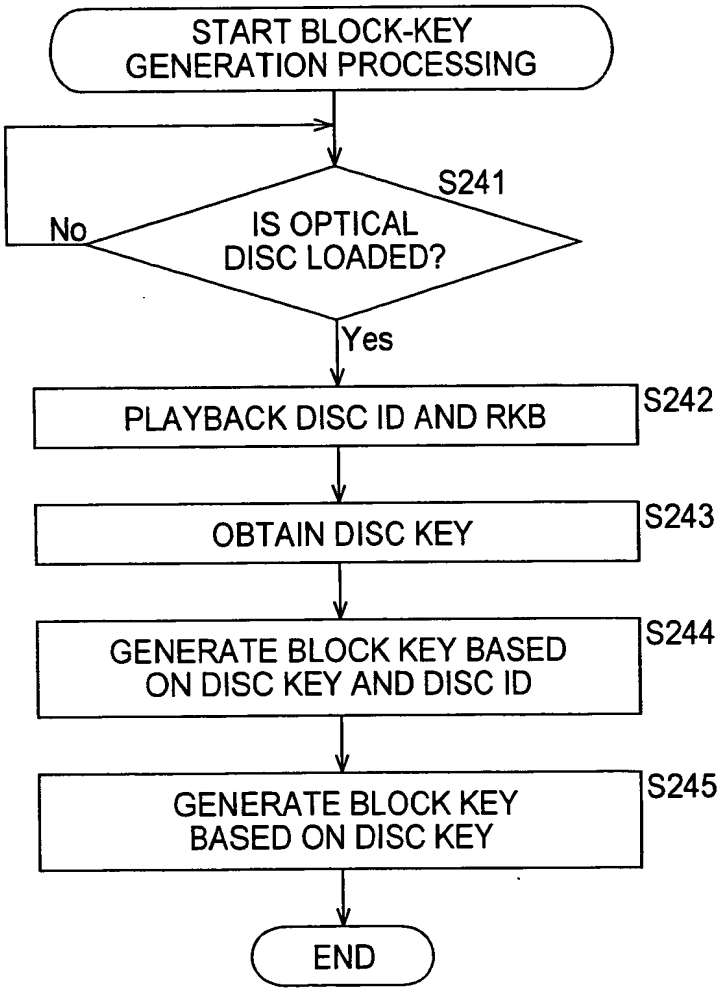

START BLOCK-KEY GENERATION PROCESSING
S241
No
IS OPTICAL DISC LOADED?
Yes
PLAYBACK DISC ID AND RKB
S242
OBTAIN DISC KEY
S243
GENERATE BLOCK KEY BASED ON DISC KEY AND DISC ID
S244
GENERATE BLOCK KEY BASED ON DISC KEY
S245
END

FIG. 27

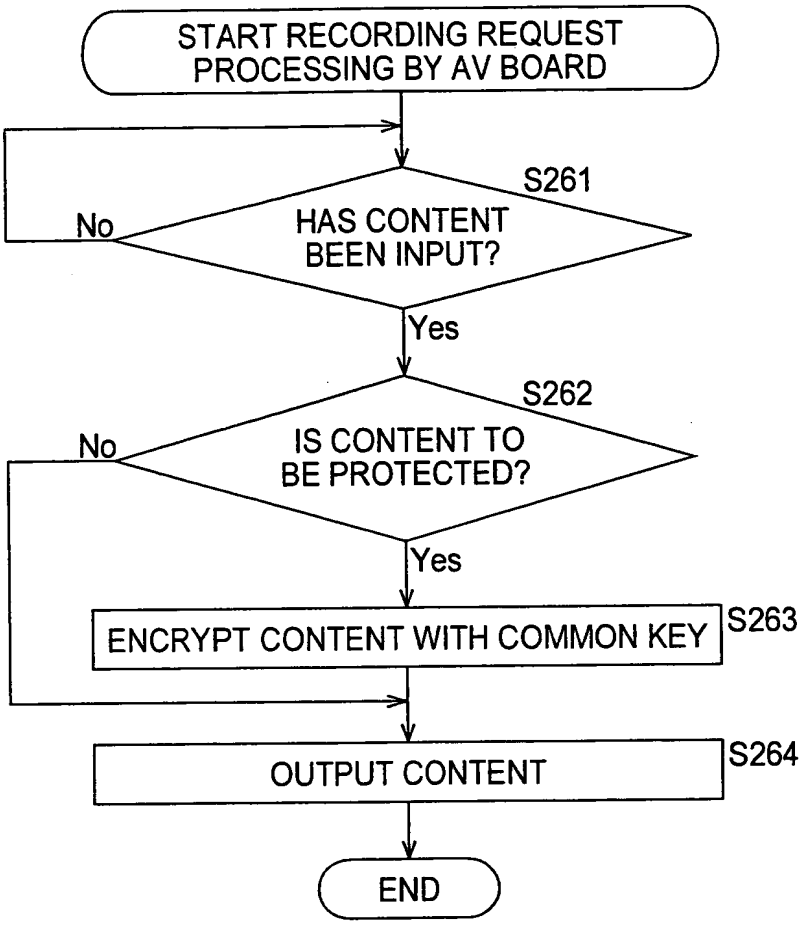

START RECORDING REQUEST PROCESSING BY AV BOARD
S261
HAS CONTENT BEEN INPUT?
No
Yes
S262
IS CONTENT TO BE PROTECTED?
No
Yes
ENCRYPT CONTENT WITH COMMON KEY
S263
OUTPUT CONTENT
S264
END

FIG. 28

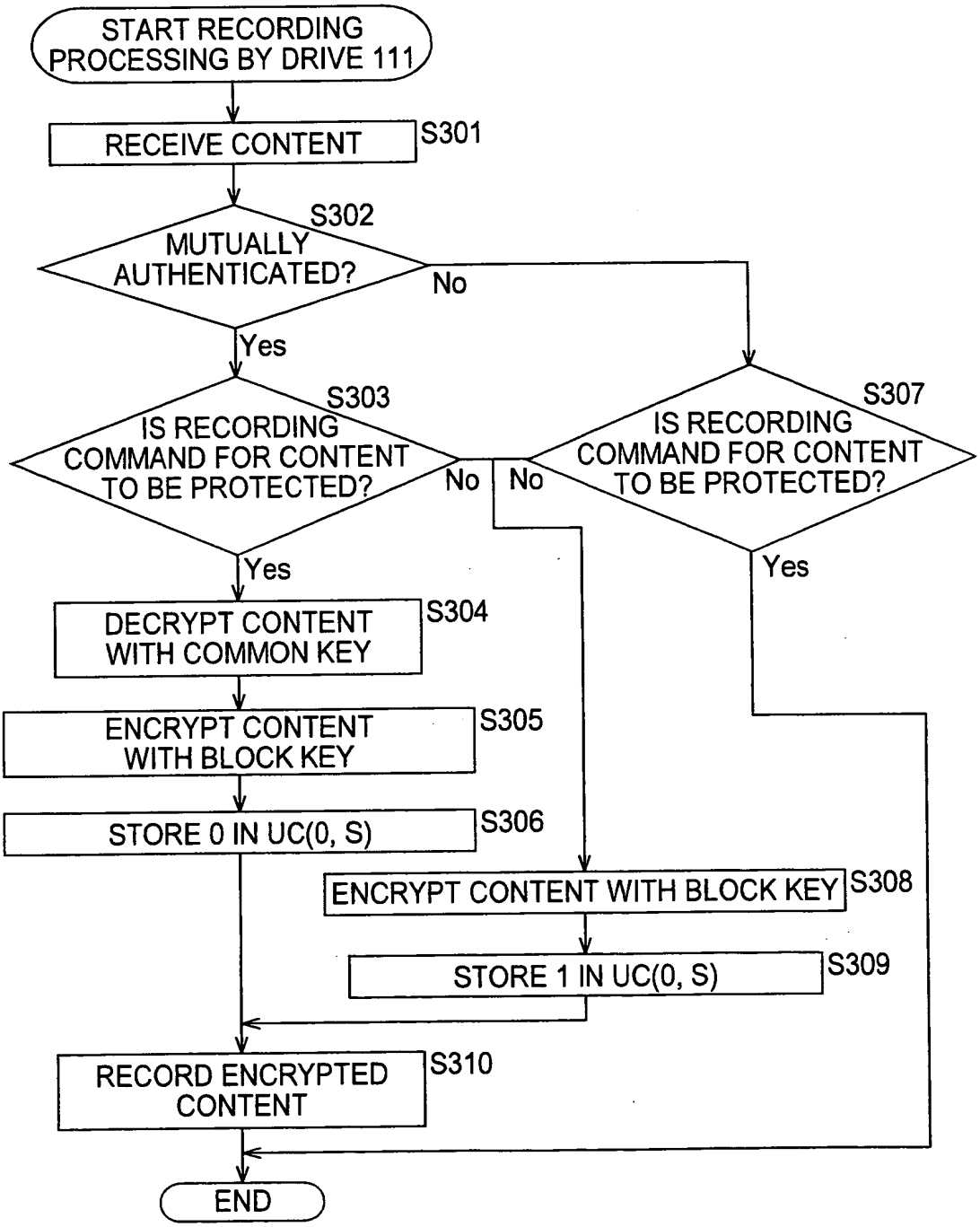

START RECORDING PROCESSING BY DRIVE 111
RECEIVE CONTENT
S301
S302
MUTUALLY AUTHENTICATED?
No
Yes
S303
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
S307
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
DECRYPT CONTENT WITH COMMON KEY
S304
ENCRYPT CONTENT WITH BLOCK KEY
S305
STORE 0 IN UC(0, S)
S306
ENCRYPT CONTENT WITH BLOCK KEY
S308
STORE 1 IN UC(0, S)
S309
RECORD ENCRYPTED CONTENT
S310
END

FIG. 29

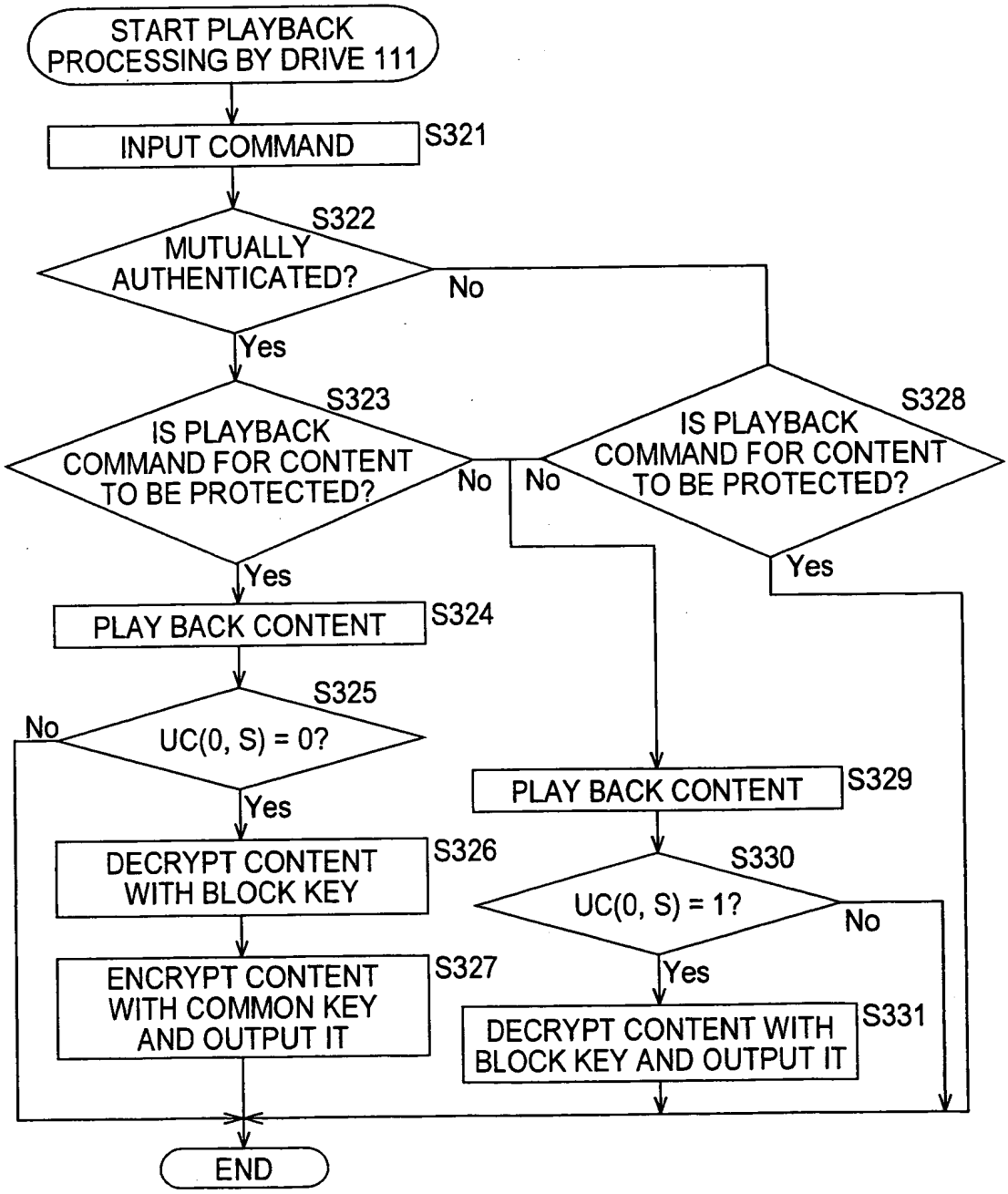

START PLAYBACK PROCESSING BY DRIVE 111
INPUT COMMAND
S321
MUTUALLY AUTHENTICATED?
S322
No
Yes
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
S323
No
Yes
PLAY BACK CONTENT
S324
UC(0, S) = 0?
S325
No
Yes
DECRYPT CONTENT WITH BLOCK KEY
S326
ENCRYPT CONTENT WITH COMMON KEY AND OUTPUT IT
S327
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
S328
No
Yes
PLAY BACK CONTENT
S329
UC(0, S) = 1?
S330
No
Yes
DECRYPT CONTENT WITH BLOCK KEY AND OUTPUT IT
S331
END

FIG. 30

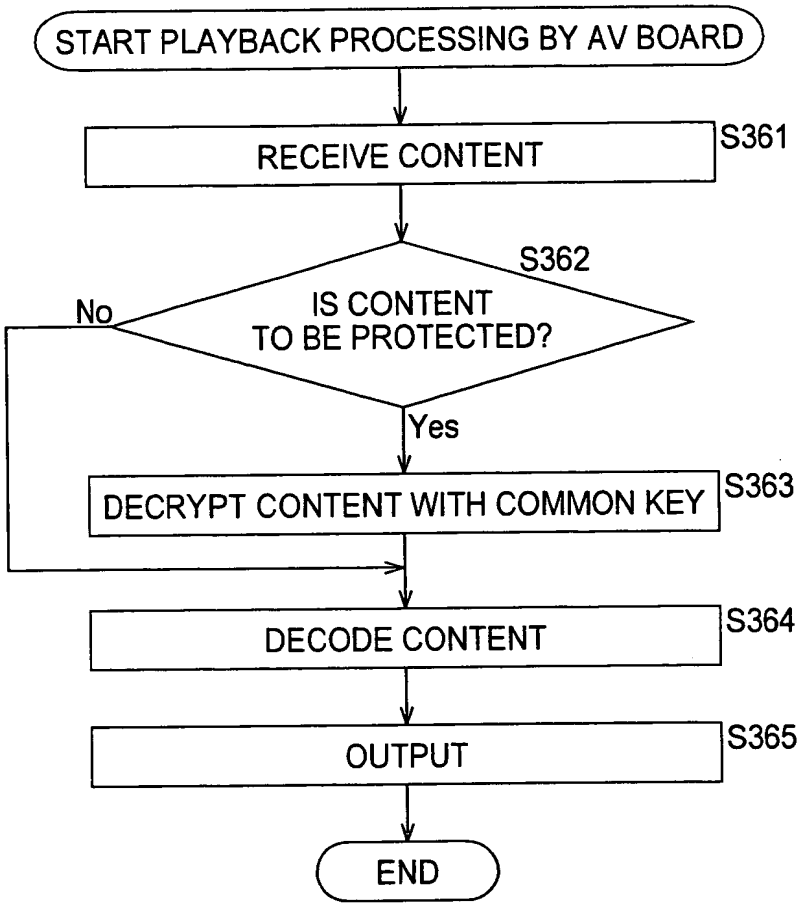

START PLAYBACK PROCESSING BY AV BOARD
RECEIVE CONTENT
S361
S362
IS CONTENT TO BE PROTECTED?
No
Yes
DECRYPT CONTENT WITH COMMON KEY
S363
DECODE CONTENT
S364
OUTPUT
S365
END

FIG. 31

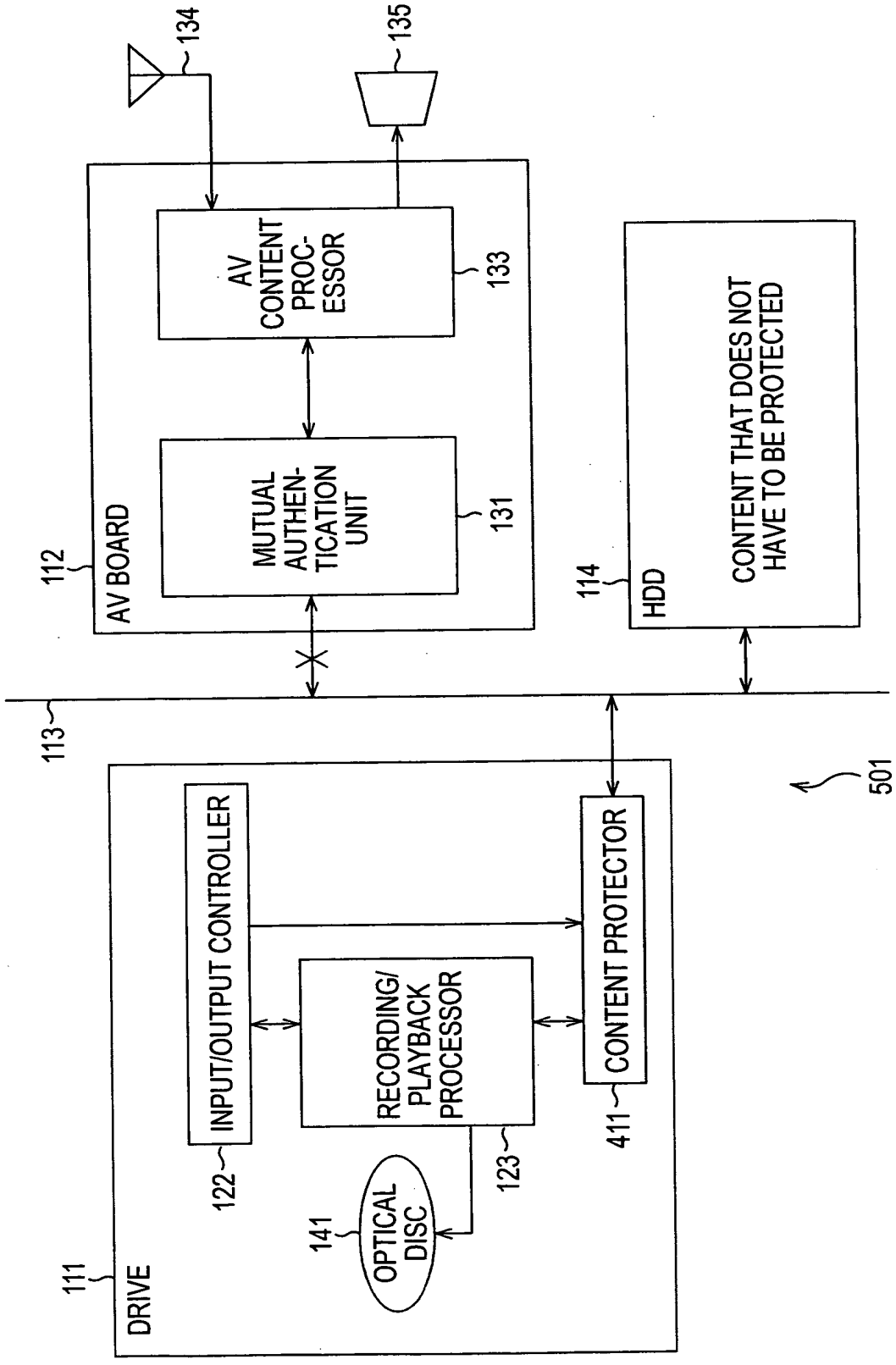

134
135
AV CONTENT PROC-ESSOR
133
MUTUAL AUTHEN-TICATION UNIT
131
112
AV BOARD
114
HDD
CONTENT THAT DOES NOT HAVE TO BE PROTECTED
113
501
INPUT/OUTPUT CONTROLLER
RECORDING/ PLAYBACK PROCESSOR
CONTENT PROTECTOR
122
123
411
141
OPTICAL DISC
111
DRIVE

FIG. 32

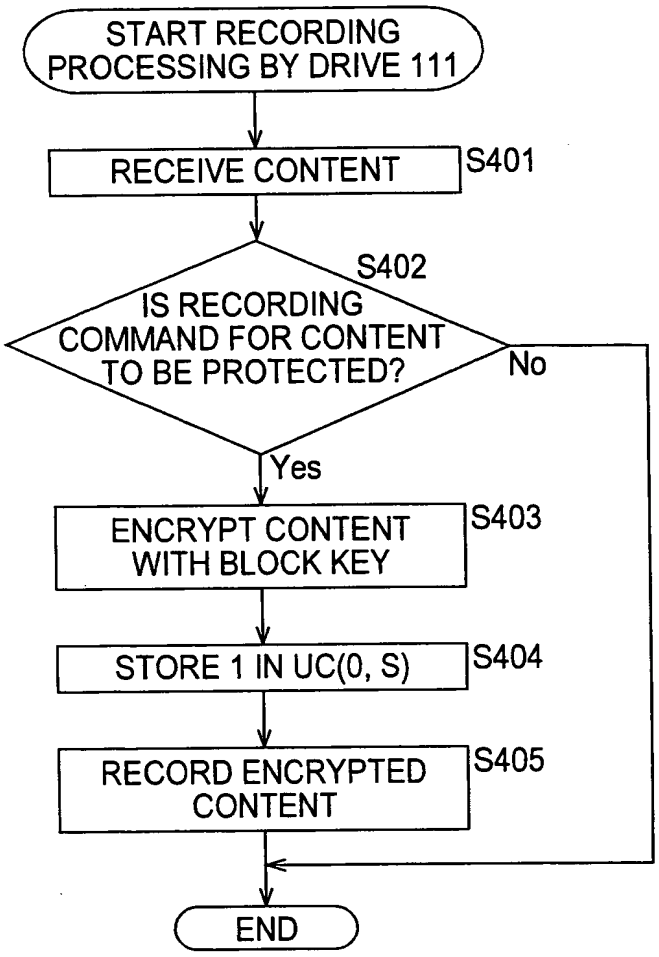

START RECORDING PROCESSING BY DRIVE 111
RECEIVE CONTENT
S401
S402
IS RECORDING COMMAND FOR CONTENT TO BE PROTECTED?
No
Yes
ENCRYPT CONTENT WITH BLOCK KEY
S403
STORE 1 IN UC(0, S)
S404
RECORD ENCRYPTED CONTENT
S405
END

FIG. 33

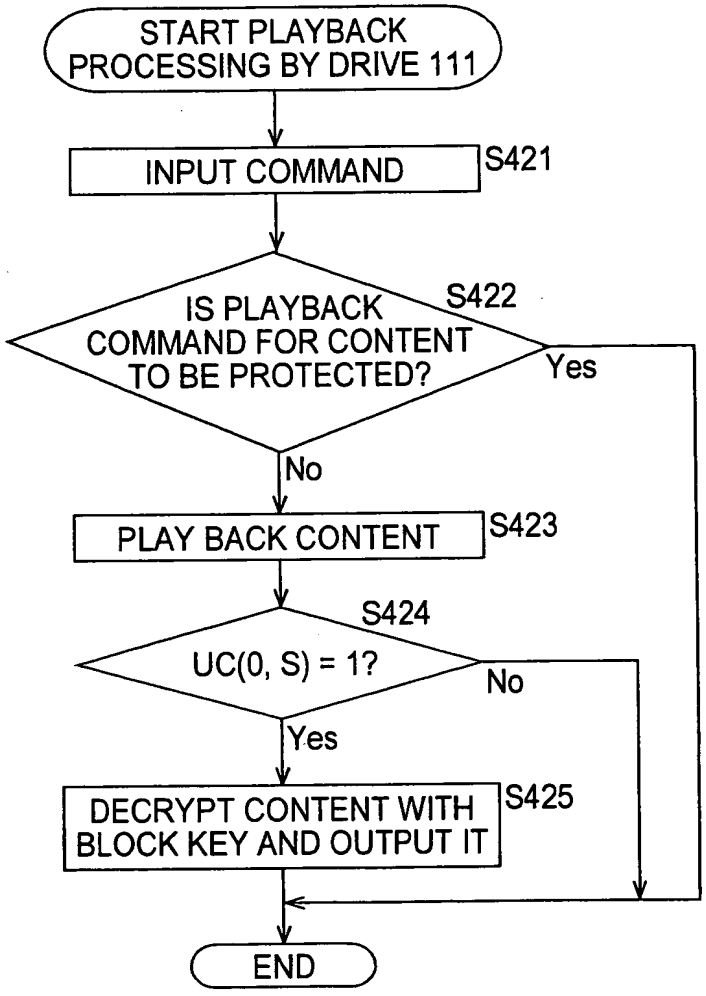
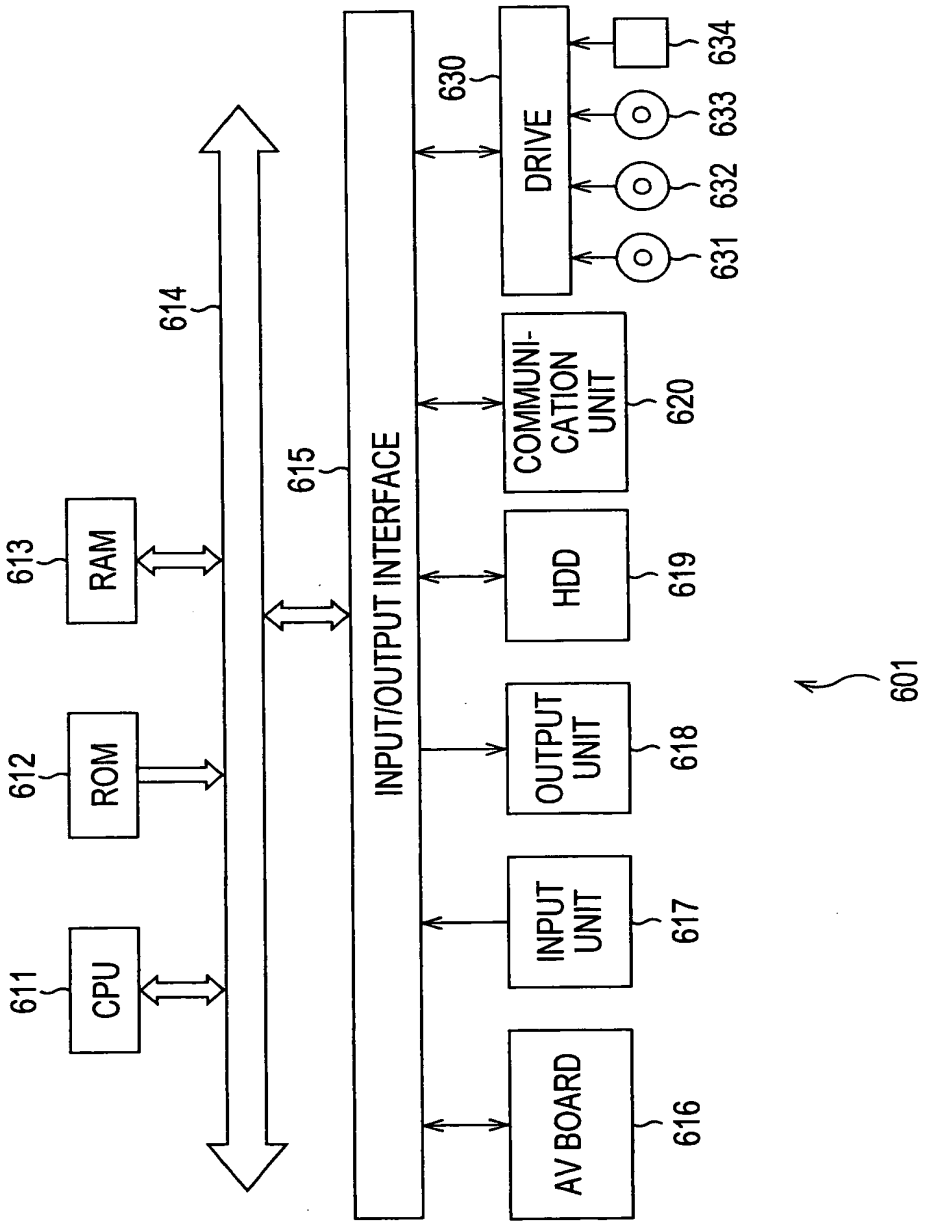

START PLAYBACK PROCESSING BY DRIVE 111
INPUT COMMAND
S421
IS PLAYBACK COMMAND FOR CONTENT TO BE PROTECTED?
S422
Yes
No
PLAY BACK CONTENT
S423
S424
UC(0, S) = 1?
No
Yes
DECRYPT CONTENT WITH BLOCK KEY AND OUTPUT IT
S425
END

FIG. 34


601
611
CPU
612
ROM
613
RAM
614
615
INPUT/OUTPUT INTERFACE
616
AV BOARD
617
INPUT UNIT
618
OUTPUT UNIT
619
HDD
620
COMMUNI-CATION UNIT
630
DRIVE
631
632
633
634